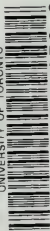


UNIVERSITY OF TORONTO



3 1761 01347273 3



G. Kyeune. Disickler

G. LEJEUNE DIRICHLET'S
WERKE.

HERAUSGEGEBEN AUF VERANLASSUNG
DER
KÖNIGLICH PREUSSISCHEN AKADEMIE DER WISSENSCHAFTEN.

IN ZWEI BÄNDEN.

BERLIN.
DRUCK UND VERLAG VON GEORG REIMER.
1889.

1898

G. LEJEUNE DIRICHLET'S WERKE.

HERAUSGEGEBEN AUF VERANLASSUNG
DER
KÖNIGLICH PREUSSISCHEN AKADEMIE DER WISSENSCHAFTEN

VON
L. KRONECKER.

ERSTER BAND.

MIT G. LEJEUNE DIRICHLET'S BILDNISS.

BERLIN.
DRUCK UND VERLAG VON GEORG REIMER.
1889.

35745

29/5/90

Yv.F. 6

QA

3

L 34

Bd. 1

VORWORT.

Es war anfangs meine Absicht, die sämmtlichen von DIRICHLET selbst veröffentlichten Arbeiten, welche in dieser Ausgabe seiner Werke die erste Abtheilung bilden sollen, in einem Bande zu vereinigen. Aber ein solcher wäre, wie sich erst beim weiteren Fortschreiten des nicht raumsparenden Druckes zeigte, für den Handgebrauch zu umfangreich geworden. Der Band musste deshalb schon vor Beendigung der ersten Abtheilung an einer geeigneten Stelle förmlich abgeschlossen werden; er enthält nunmehr, grossen Theils in chronologischer Folge, alle Arbeiten, welche DIRICHLET vor 1843, also vor seiner italienischen Reise, veröffentlicht hat, sowie den im Monatsbericht der hiesigen Akademie vom März 1846 erschienenen Aufsatz „Zur Theorie der complexen Einheiten“, welcher sich gedanklich unmittelbar an die drei vorhergehenden Arbeiten anreihet. Diesen Aufsatz hat DIRICHLET zwar erst ein Jahr nach seiner Rückkehr aus Italien in der Akademie gelesen, aber die ebenso grundlegenden als weittragenden Untersuchungen, über welche er darin „einige Mittheilungen machte“, hatte er — wie ich aus seinem eigenen Munde weiss — bereits während seines Aufenthaltes in Italien vollständig zu Ende geführt.

Die Abhandlung „*Mémoire sur l'impossibilité de quelques Équations indéterminées du cinquième degré*“, mit welcher der Band beginnt, ist typographisch getreu nach einem Exemplar abgedruckt, welches sich in DIRICHLET'S Nachlass vorgefunden hat. Dieses zeigt vielfach redactionelle Abweichungen von der unter demselben Titel im CRELLESchen Journal veröffentlichten, im vorliegenden Bande an zweiter Stelle abgedruckten Abhandlung, enthält den Text

aber wahrscheinlich genau so, wie er im Jahre 1825 der Pariser Akademie vorgelegen hat. Gewisses lässt sich freilich nicht darüber feststellen, da die Aufnahme der Abhandlung in die Sammlung der *Mémoires des Savans étrangers* nur beschlossen worden aber niemals erfolgt ist. Exemplare derselben Art, wie das erwähnte in DIRICHLET'S Nachlass, finden sich meines Wissens noch in Göttingen im Nachlass von GAUSS, hier in Berlin in der königlichen Bibliothek, in Paris in der Bibliothek des Instituts und zwar im *Fonds Huzard*. Sie tragen auf der letzten (zwanzigsten) Seite den Vermerk: „*Imprimerie de Huzard-Courcier, Rue du Jardinet n° 12*“. Ueber ihre Entstehungsweise habe ich aber noch nicht vollständige Aufklärung erlangen können. Was ich darüber in Erfahrung gebracht habe, werde ich in den Anmerkungen im zweiten Bande mittheilen, namentlich alle Ergebnisse der Akten der Pariser *Académie des Sciences*, welche deren beständiger Secretar, Herr BERTRAND, mit gewohnter Sorgfalt ermittelt und mit freundlichster Bereitwilligkeit zu meiner Verfügung gestellt hat, sowie ferner einige werthvolle Notizen, welche ich den Herren ERNST SCHERING in Göttingen und JULES TANNERY in Paris verdanke.

Bei der Herausgabe dieses Bandes hat mich Herr LAMPE auf's Wirkksamste unterstützt, ferner bei der Textrevision der sämmtlichen (mehr als fünfzig Bogen füllenden) französischen Arbeiten auch Herr MOLK, und mein verehrter Freund, Herr HERMITE, hat die grosse Güte gehabt, mit seinem Kennerblick jeden einzelnen der französischen Correcturbogen durchzusehen. Ausserdem habe ich mich bei der Revision von Originaltexten und Correcturbogen noch der gefälligen Mithülfe der Herren HENSEL, HETTNER und SCHWERING erfreut, und auch die Herren GUTZMER, RICHARD MÜLLER und SCHRENTZEL haben mir in den Angelegenheiten der Herausgabe bereitwilligst Beistand geleistet.

Es ist mir eine angenehme Pflicht den genannten Herren an dieser Stelle meinen wärmsten Dank auszusprechen.

Berlin, den 14. October 1889.

L. KRONECKER.

INHALTS - VERZEICHNISS.

	Seite
I. Mémoire sur l'impossibilité de quelques Équations indéterminées du cinquième degré.	1
Lu à l'Académie Royale des Sciences (Institut de France), le 11 juillet 1825.	
Abgedruckt nach einem Exemplare, welches sich in LEJERSE DIRICHLET'S Nachlass vorgefunden hat.	
II. Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré.	21
Lu à l'Académie Royale des Sciences (Institut de France), le 11 juillet 1825.	
CELLE, Journal für die reine und angewandte Mathematik, Bd. 3, S. 354—375. (1828.)	
III. De formis linearibus, in quibus continentur divisores primi quarumdam formularum graduum superiorum commentatio.	47
quam ad veniam docendi ab amplissimo philosophorum ordine in regia universitate litterarum Vratislaviensi impetrandam conscripsit GUSTAVS LEJERSE DIRICHLET, philosophiae doctor.	
Vratislaviae, typis Kupferianis. (Wahrscheinlich 1828.)	
IV. Recherches sur les diviseurs premiers d'une classe de formules du quatrième degré.	63
CELLE, Journal für die reine und angewandte Mathematik, Bd. 3, S. 35—69. (1828.)	
V. Démonstrations nouvelles de quelques théorèmes relatifs aux nombres.	99
CELLE, Journal für die reine und angewandte Mathematik, Bd. 3, S. 390—393. (1828.)	
VI. Question d'analyse indéterminée.	105
CELLE, Journal für die reine und angewandte Mathematik, Bd. 3, S. 407—408. (1828.)	
VII. Note sur les intégrales définies.	109
CELLE, Journal für die reine und angewandte Mathematik, Bd. 4, S. 94—98. (1829.)	
VIII. Sur la convergence des séries trigonométriques qui servent à représenter une fonction arbitraire entre des limites données.	117
CELLE, Journal für die reine und angewandte Mathematik, Bd. 4, S. 157—169. (1829.)	

	Seite
IX. Ueber die Darstellung ganz willkürlicher Functionen durch Sinns- und Cosinusreihen.	133
Repertorium der Physik, unter Mitwirkung der Herren LEJEUNE DIRICHLET, JACOBI, NEUMANN, RIESS, STREBLKE, herausgegeben von HEINRICH WILHELM DOVE und LUDWIG MOSEER. Bd. I, 1837, S. 152—174.	
X. Solution d'une question relative à la théorie mathématique de la chaleur. .	161
CRELLE, Journal für die reine und angewandte Mathematik, Bd. 5, S. 287—295. (1830)	
XI. Démonstration d'une propriété analogue à la loi de réciprocité qui existe entre deux nombres premiers quelconques.	173
CRELLE, Journal für die reine und angewandte Mathematik, Bd. 9, S. 379—389. (1832.)	
XII. Démonstration du théorème de Fermat pour le cas des 14 ^{èmes} puissances.	189
CRELLE, Journal für die reine und angewandte Mathematik, Bd. 9, S. 390—393. (1832.)	
XIII. Untersuchungen über die Theorie der quadratischen Formen.	195
Abhandlungen der Königlich Preussischen Akademie der Wissenschaften von 1833, S. 101—121.	
XIV. Einige neue Sätze über unbestimmte Gleichungen.	219
Abhandlungen der Königlich Preussischen Akademie der Wissenschaften von 1834, S. 649—664.	
XV. Ueber eine neue Anwendung bestimmter Integrale auf die Summation endlicher oder unendlicher Reihen.	237
Abhandlungen der Königlich Preussischen Akademie der Wissenschaften von 1835, S. 391—407.	
XVI. Sur l'usage des intégrales définies dans la sommation des séries finies ou infinies.	257
CRELLE, Journal für die reine und angewandte Mathematik, Bd. 17, S. 57—67. (1837.)	
XVII. Sur les intégrales Eulériennes.	271
CRELLE, Journal für die reine und angewandte Mathematik, Bd. 15, S. 258—263. (1836.)	
XVIII. Ueber die Methode der kleinsten Quadrate.	279
Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1836, S. 67—68.	
XIX. Sur les séries dont le terme général dépend de deux angles, et qui servent à exprimer des fonctions arbitraires entre des limites données.	283
CRELLE, Journal für die reine und angewandte Mathematik, Bd. 17, S. 35—56. (1837.)	
XX. Beweis eines Satzes über die arithmetische Progression.	307
Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1837, S. 108—110.	
XXI. Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält.	313
Abhandlungen der Königlich Preussischen Akademie der Wissenschaften von 1837, S. 45—81.	

	Seite
XXII. Sur la manière de résoudre l'équation $t^2 - pu^2 = 1$ au moyen des fonctions circulaires.	343
(CRELLE, Journal für die reine und angewandte Mathematik, Bd. 17, S. 286—290. (1837.))	
XXIII. Ueber die Bestimmung asymptotischer Gesetze in der Zahlentheorie.	351
Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1838, S. 13—15.	
XXIV. Sur l'usage des séries infinies dans la théorie des nombres.	357
(CRELLE, Journal für die reine und angewandte Mathematik, Bd. 18, S. 259—274. (1838.))	
XXV. Sur une nouvelle méthode pour la détermination des intégrales multiples.	375
Comptes rendus hebdomadaires des séances de l'Académie des Sciences. Tome VIII, p. 156—160. (1839.)	
(LIOUVILLE, Journal de Mathématiques, Sér. I, Tome IV, p. 164—168.)	
XXVI. Ueber eine neue Methode zur Bestimmung vielfacher Integrale.	381
Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1839, S. 18—25.	
XXVII. Ueber eine neue Methode zur Bestimmung vielfacher Integrale.	391
Abhandlungen der Königlich Preussischen Akademie der Wissenschaften von 1839, S. 61—79.	
XXVIII. Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres.	411
(CRELLE, Journal für die reine und angewandte Mathematik, Bd. 19, S. 324—369, Bd. 21, S. 1—12 und S. 134—155. (1839, 1840.))	
XXIX. Ueber eine Eigenschaft der quadratischen Formen.	497
Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1840, S. 49—52.	
(CRELLE, Journal für die reine und angewandte Mathematik, Bd. 21, S. 98—100.)	
XXX. Untersuchungen über die Theorie der complexen Zahlen.	503
Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1841, S. 190—194.	
(CRELLE, Journal für die reine und angewandte Mathematik, Bd. 22, S. 375—378.)	
XXXI. Untersuchungen über die Theorie der complexen Zahlen.	509
Abhandlungen der Königlich Preussischen Akademie der Wissenschaften von 1841, S. 141—161.	
XXXII. Recherches sur les formes quadratiques à coefficients et à indéterminées complexes.	533
(CRELLE, Journal für die reine und angewandte Mathematik, Bd. 24, S. 291—371. (1842.))	
XXXIII. Sur la théorie des nombres.	619
Comptes rendus hebdomadaires des séances de l'Académie des Sciences, Tome X, p. 285—288. (1840.)	
(LIOUVILLE, Journal de Mathématiques, Sér. I, Tome V, p. 72—74.)	

	Seite
XXXIV. Einige Resultate von Untersuchungen über eine Classe homogener Functionen des dritten und der höheren Grade.	625
Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1841, S. 280—285.	
XXXV. Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen.	633
Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1842, S. 93—95.	
XXXVI. Zur Theorie der complexen Einheiten.	639
Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1846, S. 103—107.	

I. A B T H E I L U N G,

ENTHALTEND

DIE VON G. LEJEUNE DIRICHLET SELBST VERÖFFENTLICHTEN ARBEITEN.

MÉMOIRE

Sur l'impossibilité de quelques Équations indéterminées du cinquième degré,

LU A L'ACADÉMIE ROYALE DES SCIENCES (INSTITUT DE FRANCE), LE 11 JUILLET 1825.
PAR G. LEJEUNE DIRICHLET.

(D'après le Rapport de MM. Lacroix et Legendre, ce Mémoire a été approuvé, et doit être imprimé dans
le Recueil des Mémoires des Savans étrangers.)

(Abgedruckt nach einem Exemplare, welches sich in Lejeune Dirichlet's Nachlass vorgefunden hat.)

MÉMOIRE

Sur l'impossibilité de quelques Équations indéterminées du cinquième degré,

LU A L'ACADÉMIE ROYALE DES SCIENCES (INSTITUT DE FRANCE), LE 11 JUILLET 1825,
PAR G. LEJEUNE DIRICHLET.

(D'après le Rapport de MM. Lacroix et Legendre, ce Mémoire a été approuvé, et doit être imprimé dans le Recueil des Mémoires des Savans étrangers.)

On sait que la théorie des équations indéterminées des degrés supérieurs au second, est encore très peu avancée: il est vrai qu'il y a une infinité d'équations de tous les degrés dont on peut démontrer l'impossibilité en faisant voir que quelles que soient les valeurs que l'on attribue aux indéterminées, les deux membres de l'équation proposée ne peuvent jamais donner le même reste lorsqu'on les divise par un certain nombre ou module; mais lorsqu'une équation ne peut pas être traitée par ce moyen, il devient difficile de prouver qu'elle est impossible, et on n'y est parvenu, jusqu'à présent, que pour un très petit nombre d'équations. Toutes ces équations sont très particulières, et d'une forme telle, que lorsqu'on cherche à les résoudre, on est naturellement conduit à une ou plusieurs formules quadratiques qu'il s'agit d'égaliser à des puissances parfaites. On satisfait ensuite de la manière la plus générale à cette condition, en exprimant les indéterminées par d'autres indéterminées, dont les premières deviennent des fonctions entières, et il se trouve, du moins dans tous les cas où la méthode dont il est question réussit, que les nouvelles indéterminées ou d'autres quantités qui en dépendent d'une manière très simple, satisfont également à une équation semblable à l'équation proposée. Comme les nouvelles indéterminées sont en même temps plus petites que les indéterminées primitives, l'impossibilité de l'équation proposée se trouve établie; car il est évident que si elle était possible, on aurait le moyen d'obtenir une suite décroissante et indéfinie de nombres entiers, ce qui implique contradiction. C'est de cette

manière que Fermat et Euler ont prouvé l'impossibilité de plusieurs équations du troisième et du quatrième degré.

En essayant d'appliquer des considérations semblables à quelques équations du cinquième degré et d'une forme analogue à celles des équations traitées par Fermat et Euler, on est arrêté tout aussitôt. La formule quadratique à laquelle on arrive, et qu'il faut égaler à une cinquième puissance, admet plusieurs solutions différentes, et parmi ces solutions, il n'y en a qu'une seule qui conduise à une équation semblable à l'équation proposée. En réfléchissant à cette difficulté, j'ai reconnu qu'elle pouvait être levée très simplement en assujettissant à quelques conditions le nombre déterminé qui entre dans l'équation. Il résulte d'un théorème exposé dans les préliminaires, que lorsque ces conditions se trouvent remplies, les différentes solutions dont la formule quadratique est susceptible, en général, doivent être rejetées, à l'exception d'une seule, qui est précisément celle de laquelle on déduit des nombres qui satisfont à une équation semblable à l'équation proposée. On parvient ainsi à établir l'impossibilité d'une classe assez étendue d'équations indéterminées du cinquième degré. Le premier membre de ces équations est la somme ou la différence de deux cinquièmes puissances, et le second membre est le produit d'une cinquième puissance et d'un nombre déterminé assujéti à différentes conditions. En attribuant à ce nombre des valeurs particulières compatibles avec ces conditions, on peut obtenir autant de théorèmes particuliers que l'on veut. Cette généralité de nos théorèmes est d'autant plus singulière, que les équations analogues du troisième et du quatrième degré, dont l'impossibilité a été démontrée jusqu'à présent, ne sont qu'en nombre fini et même très petit.

Les nombres P et Q devant être premiers entre eux, l'un pair, l'autre impair, et le premier de plus non-divisible par 5, on peut démontrer que, pour égaler le binôme $P^2 - 5Q^2$ à une cinquième puissance avec toute la généralité convenable, on n'a qu'à poser

$$P + Q\sqrt{5} = (M \pm N\sqrt{5})^5 (t \pm u\sqrt{5}),$$

les parties rationnelles et les coefficients de $\sqrt{5}$ étant égalés séparément, t et u satisfaisant généralement à l'équation $t^2 - 5u^2 = 1$, et les nombres M et N étant premiers entre eux, l'un pair, l'autre impair, et le premier non-divisible

par 5 (*). Cela supposé, il n'est pas difficile d'établir le théorème que nous allons énoncer.

Théorème I.

«Les nombres P et Q devant être premiers entre eux, l'un pair, l'autre impair, et le dernier devant être de plus divisible par 5, je dis que pour égaliser le binome $P^2 - 5Q^2$ de la manière la plus générale à une cinquième puissance, il suffira de poser

$$P+Q\sqrt{5} = (g + \psi\sqrt{5})^5.$$

«Les indéterminées g et ψ étant premières entre elles, l'une paire, l'autre impaire, et la première de plus non-divisible par 5 (**).»

Pour égaliser $P^2 - 5Q^2$ à une cinquième puissance, nous poserons, d'après ce qui vient d'être dit,

$$P+Q\sqrt{5} = (M \pm N\sqrt{5})^5 (t \pm u\sqrt{5}).$$

• N n'étant pas divisible par 5, si nous faisons pour un instant

$$(M+N\sqrt{5})^5 = M' + N'\sqrt{5},$$

il sera facile de voir que N' est divisible par 5, et que M' ne l'est pas. En substituant l'expression précédente dans la valeur de $P+Q\sqrt{5}$, on aura

$$P+Q\sqrt{5} = (M' \pm N'\sqrt{5})(t \pm u\sqrt{5}),$$

d'où l'on tire

$$Q = \pm M'u \pm N't.$$

N' étant divisible par 5, et M' ne l'étant pas, il est évident que Q ne pourra être divisible par 5, qu'autant que u le sera. Les valeurs les plus petites qui satisfont à l'équation

$$t^2 - 5u^2 = 1,$$

sont celles-ci,

$$t = 9, \quad u = 4.$$

(*) Pour ne pas donner trop d'étendue à ce Mémoire, je supprime ici une première partie du mémoire manuscrit contenant quelques théorèmes sur les nombres en tant qu'ils sont de la forme $t^2 - au^2$, et la démonstration de la proposition dont il s'agit, fondée sur ces théorèmes.

(**) Il n'est peut-être pas inutile de faire remarquer qu'il y a des théorèmes analogues pour beaucoup d'autres nombres premiers, et que pour les établir, on peut faire usage des mêmes considérations dont nous nous servons ici.

Les valeurs générales seront par conséquent données par cette formule,

$$t+u\sqrt{5} = (9+4\sqrt{5})^p,$$

dans laquelle p est un nombre entier, positif quelconque (*): on tire de là

$$u = \frac{p}{1} 9^{p-1} \cdot 4 + \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3} 9^{p-3} \cdot 4^3 \cdot 5 + \text{etc.}$$

Tous les termes de cette valeur, à partir du second, étant divisibles par 5, quel que soit p , on voit que pour que u puisse être divisible par 5, il faut que le premier terme, et par conséquent aussi p , soit divisible par 5. Si nous faisons donc $p = 5p'$, p' étant un entier, et que nous substituions la valeur de $t+u\sqrt{5}$ dans celle de $P+Q\sqrt{5}$, nous aurons

$$P+Q\sqrt{5} = (M \pm N\sqrt{5})^5 (9 \pm 4\sqrt{5})^{5p'},$$

résultat qui, par l'introduction des nouvelles indéterminées, g et ψ qui sont telles que

$$(M \pm N\sqrt{5})(9 \pm 4\sqrt{5})^{p'} = g + \psi\sqrt{5},$$

se change en celui-ci,

$$P+Q\sqrt{5} = (g + \psi\sqrt{5})^5.$$

La forme de la solution donnée par l'énoncé du théorème se trouvant ainsi justifiée, il ne reste plus qu'à déterminer la nature des indéterminées.

Comme on a

$$P^2 - 5Q^2 = (g^2 - 5\psi^2)^5,$$

et que les nombres P et Q sont respectivement divisibles par g et ψ , on voit facilement que les indéterminées g et ψ doivent être supposées premières entre elles, l'une paire, l'autre impaire, et la première de plus non-divisible par 5. On peut même ajouter que g ou ψ sera impaire selon que P et Q l'est. Réciproquement, si les indéterminées g et ψ satisfont aux conditions précédentes, les nombres P et Q déterminés par la formule

$$P+Q\sqrt{5} = (g + \psi\sqrt{5})^5,$$

seront premiers entre eux, comme il est facile de s'en assurer. Ces préliminaires établis, nous pourrions nous occuper des théorèmes qui font l'objet principal de ce Mémoire. Le premier de ces théorèmes peut s'énoncer de la manière suivante.

(*) Voyez les Additions à l'Algèbre d'Euler (art. 75), ou les *Disquisitiones arithmeticae* (art. 200).

Théorème II.

Les nombres m et n étant positifs, plus grands que zéro, et le second de plus différent de 2, et le nombre A n'étant divisible ni par 2 ni par 5, ni par aucun nombre premier de l'une de ces formes $10k \pm 1$ (*), il sera impossible de trouver deux nombres x et y premiers entre eux, tels que $x^5 \pm y^5 = 2^m 5^n A z^5$ (a).⁴

Supposons, contre l'énoncé du théorème, que l'équation soit possible. Comme le second membre est pair (m ayant été supposé > 0), il faut que les nombres x et y , qui sont premiers entre eux, soient impairs l'un et l'autre. Si nous faisons $x \pm y = 2p$, $x \mp y = 2q$, et par suite,

$$x = p + q, \quad \pm y = p - q,$$

les nombres p et q seront entiers, premiers entre eux, et de plus l'un pair, l'autre impair. En substituant les valeurs précédentes de x et $\pm y$ dans l'équation (a), on la changera en celle-ci:

$$2p(p^4 + 10p^2q^2 + 5q^4) = 2^m 5^n A z^5.$$

Le premier membre ne peut être égal au second membre, qui est divisible par 5, qu'autant qu'on suppose p divisible par 5. Faisant donc $p = 5r$, nous aurons

$$2.5^2 r(q^4 + 2.5^2 q^2 r^2 + 5^3 r^4) = 2^m 5^n A z^5.$$

Le nombre n est par hypothèse égal à l'unité ou plus grand que 2. Si n est égal à l'unité, il faudra, dans l'équation précédente, supposer z divisible par 5. On pourra, dans ce cas, mettre $5z$ à la place de z , ou, ce qui est la même chose, donner à 5 l'exposant 6, d'où l'on voit que l'on peut supposer dans tous les cas, que $n > 2$. Si l'on met maintenant l'équation précédente sous cette forme.

$$r(q^4 + 2.5^2 q^2 r^2 + 5^3 r^4) = 2^{m-1} 5^{n-2} A z^5,$$

(*) Les théorèmes de ce Mémoire, de même que ceux qui sont contenus dans l'addition, sont susceptibles d'une extension que je vais indiquer en deux mots. Ces théorèmes ont encore lieu quand même A aurait des diviseurs premiers de la forme $10k - 1$. On verra en effet que notre démonstration suppose uniquement que le nombre A ne puisse avoir aucun diviseur commun avec la formule $t^4 + 10t^2s^2 + 5s^4$, t et s étant supposés premiers entre eux. Or, cette formule pouvait se mettre sous la forme $\frac{(t+s)^5 + (t-s)^5}{2t}$, et le nombre 5 étant premier, il résulte des théorèmes connus d'Euler sur les formes linéaires des diviseurs premiers de l'expression $x^n \pm y^n$, que notre formule n'a que des diviseurs premiers de la forme $10k + 1$, et est par conséquent première à A . Voyez la Théorie des nombres ou le Mémoire d'Euler, *circa divisores numerorum*, dans le 1^{er} vol. des *Novi Acad. Comment. Petrop.*

et qu'on se rappelle que les nombres q et $p = 5r$, sont premiers entre eux, et de plus, l'un pair, l'autre impair, il sera facile de voir que le facteur trinome est impair, non-divisible par 5, et premier à r : il faut donc que r soit divisible par 5, n étant ≥ 2 . Choisissons actuellement deux nombres positifs, μ et ν , tels que (*) $m + \mu - 1$, $n + \nu - 2$, soient divisibles par 5, et un nombre B qui n'ait d'autres diviseurs premiers que le nombre A, et tel que le produit AB soit une cinquième puissance. Si nous multiplions l'équation précédente par $2^\mu 5^\nu B$, nous aurons celle-ci:

$$2^\mu 5^\nu B r (q^4 + 2 \cdot 5^2 q^2 r^2 + 5^3 r^4) = 2^{m+\mu-1} 5^{n+\nu-2} A B^5.$$

Le second membre de cette équation étant une cinquième puissance, le premier membre en sera pareillement une. Or, je dis que les deux facteurs dans lesquels ce premier membre peut se décomposer, le facteur $2^\mu 5^\nu B r$ et le facteur trinome, sont premiers entre eux. En effet, nous avons déjà vu plus haut que le facteur trinome est premier à $2^\mu 5^\nu r$, et pour s'assurer qu'il est également premier à B, on le mettra sous cette forme,

$$(q^2 + 5^2 r^2)^2 - 5(10r^2)^2.$$

Les nombres $q^2 + 5^2 r^2$ et $10r^2$ étant évidemment premiers entre eux, tout nombre premier par lequel le facteur trinome est divisible, sera de l'une de ces deux formes, $10k \pm 1$, dont aucune ne convient par hypothèse aux nombres premiers diviseurs de A, et par conséquent aussi de B, B n'ayant pas d'autres diviseurs premiers que A. Il faut donc que le nombre $2^\mu 5^\nu B r$ et le facteur trinome soient des cinquièmes puissances l'un et l'autre.

Le facteur trinome pouvant s'écrire de cette manière,

$$(q^2 + 5^2 r^2)^2 - 5(10r^2)^2,$$

et les nombres $q^2 + 5^2 r^2$, $10r^2$ étant premiers entre eux, le premier impair et le second pair et divisible par 5, il suffira, en vertu du théorème I, pour égaliser le facteur trinome avec toute la généralité convenable à une cinquième puissance, de poser ces deux équations,

$$\begin{aligned} q^2 + 5^2 r^2 &= t(t^4 + 2 \cdot 5^2 t^2 s^2 + 5^3 s^4), \\ 10r^2 &= 5s(t^4 + 10t^2 s^2 + 5s^4). \end{aligned}$$

(*) Si $m - 1$ était divisible par 5, on choisirait pour μ une autre valeur que zéro pour éviter les exposans négatifs dans ce qui va suivre.

Les nombres s et t doivent être supposés premiers entre eux, et de plus le premier pair et le second impair et non-divisible par 5. Il suit de là que s doit être divisible par 5: en effet t n'étant pas divisible par 5, le second membre de la seconde équation ne peut être divisible par 5^2 qu'autant que s est divisible par 5: mais le premier membre qui a ν^2 pour facteur, est divisible par 5^2 : donc s est divisible par 5.

Nous avons vu plus haut que $2^u 5^t B\nu$ devait être une cinquième puissance. Le nombre $2^{2u} 5^{2t} B^2 \nu^2$, carré du nombre précédent, devra donc être une puissance du même degré, et même du dixième degré. Or, en multipliant par $2^{2u-1} 5^{2t-1} B^2$ les deux membres de la dernière équation, on aura celle-ci:

$$2^{2u-1} 5^{2t-1} B^2 \nu^2 = 2^{2u-1} 5^{2t} B^2 s(t^4 + 10t^2 s^2 + 5s^4).$$

Si donc nous faisons pour abrégér: $2u-1 = g$, $2\nu = h$, $B^2 = C$, tout se réduira à faire voir qu'il est impossible de trouver deux nombres s et t premiers entre eux, et dont le premier soit de plus pair et divisible par 5, tels que le produit

$$2^g 5^h C s(t^4 + 10t^2 s^2 + 5s^4) \quad (\beta)$$

soit une cinquième puissance.

En ayant égard à la nature des diviseurs premiers de C , on s'assurera facilement que le facteur $2^g 5^h C s$ et le facteur trinôme sont premiers entre eux. Il faudrait donc, pour que le produit (β) pût être une cinquième puissance, que chacun de ces facteurs en fût pareillement une. Le facteur trinôme peut s'écrire de cette manière:

$$(t^2 + 5s^2)^2 - 5(2s^2)^2.$$

Comme les nombres $t^2 + 5s^2$, $2s^2$ sont évidemment premiers entre eux, et de plus le premier impair et le second pair et divisible par 5, le théorème I est applicable ici, et l'on pourra poser

$$\begin{aligned} t^2 + 5s^2 &= t'(t'^4 + 2 \cdot 5^2 t'^2 s'^2 + 5^3 s'^4) \\ 2s^2 &= 5s'(t'^4 + 10t'^2 s'^2 + 5s'^4). \end{aligned}$$

Les nombres s' et t' doivent être supposés premiers entre eux, et de plus le premier pair et le second impair et non-divisible par 5. Comme t' n'est pas divisible par 5, il est évident par la seconde équation, dont le premier membre renferme le facteur s'^2 , et est par conséquent divisible par 5^2 , que s'

doit être divisible par 5. Ainsi les nombres s' et t' sont premiers entre eux, de même que les nombres s et t , et le premier s' est en outre pair et divisible par 5 comme s .

Il est facile encore de voir que s' est plus petit que s ; car on conclut immédiatement de la dernière équation $5^2 s'^5 < 2 s^2$ et par suite $s' < \sqrt[5]{\frac{2s^2}{5}}$.

On a vu plus haut que $2^g 5^h C s$ devait être une cinquième puissance. Le nombre $2^{2g} 5^{2h} C^2 s^2$, carré du précédent, devra donc être une puissance du même degré. Or, en multipliant les deux membres de la dernière équation par $2^{2g-1} 5^{2h} C^2$, on aura

$$2^{2g} 5^{2h} C^2 s^2 = 2^{2g-1} 5^{2h+1} C^2 s' (t'^4 + 10 t'^2 s'^2 + 5 s'^4),$$

ou ce qui est la même chose en faisant $2g-1 = g'$, $2h+1 = h'$, $C^2 = C'$, dans le second membre,

$$2^{2g} 5^{2h} C^2 s^2 = 2^{g'} 5^{h'} C' s' (t'^4 + 10 t'^2 s'^2 + 5 s'^4). \quad (\beta')$$

équation dont les deux membres doivent être des puissances du cinquième degré.

Nous voilà donc arrivés à un produit (β') semblable au produit (β) , mais dans lequel le nombre s' est plus petit que le nombre s du produit (β) , et ce produit (β') serait une cinquième puissance, si le produit (β) en était une. En traitant le produit (β') comme nous avons traité le produit (β) , on arriverait à un troisième produit (β'') , dans lequel le nombre s'' serait plus petit que s' , et l'on pourrait continuer ce procédé aussi loin que l'on voudrait. Il est facile de voir en outre que quelque loin que l'on prolonge les séries $s, s', s'', \dots; t, t', t'', \dots$ on ne pourra jamais rencontrer un terme égal à zéro; car il est évident que si l'on supposait nul un de ces termes, on conclurait en remontant que $s = 0$, cas évident, et qui d'ailleurs est exclu, puisque les nombres s et t ont été supposés premiers entre eux.

Si donc le produit (β) pouvait être une cinquième puissance, on pourrait obtenir, par l'analyse précédente, une suite indéfinie de nombres entiers positifs, dans laquelle chaque terme serait plus petit que le terme précédent, sans qu'aucun des termes ne fût nul; ce qui implique contradiction. On doit conclure de là que le produit (β) ne saurait être une puissance du cinquième degré.

Le théorème II se trouvant ainsi établi, nous allons donner le moyen d'en déduire un autre théorème plus général. Considérons l'équation

$$x^5 \pm y^5 = 2^m \Lambda z^5,$$

dans laquelle nous supposons x et y premiers entre eux, $m > 0$, et Λ soumis aux mêmes restrictions que dans l'énoncé du théorème II. Soient α, β, γ des nombres positifs moindres que 5, et tels que $x \equiv \alpha, \pm y \equiv \beta, z \equiv \gamma \pmod{5}$ et soit encore H un nombre positif ≤ 25 et tel que $2^m \Lambda \equiv H \pmod{25}$. Comme 5 est un nombre premier, on aura

$$x^5 \equiv \alpha, \quad y^5 \equiv \beta, \quad z^5 \equiv \gamma, \quad (\text{mod } 5).$$

On conclut de là, en ayant égard à l'équation posée plus haut,

$$x \pm y \equiv 2^m \Lambda z \pmod{5},$$

et partant

$$\alpha + \beta \equiv H\gamma \pmod{5}.$$

Comme α est le reste de x , on pourra poser $x = \alpha + 5k$, k étant un entier; on tire de là, en élevant les deux membres à la cinquième puissance,

$$x^5 = \alpha^5 + 5\alpha^4(5k) + \frac{5 \cdot 4}{1 \cdot 2} \alpha^3(5k)^2 + \text{etc.},$$

et on aura donc

$$x^5 \equiv \alpha^5 \pmod{25}.$$

On trouvera de la même manière $\pm y^5 \equiv \beta^5, z^5 \equiv \gamma^5 \pmod{25}$, et comme on a aussi $2^m \Lambda \equiv H \pmod{25}$, on trouvera, en ayant égard à l'équation citée,

$$\alpha^5 + \beta^5 \equiv H\gamma^5 \pmod{25}.$$

Si maintenant, en substituant dans cette congruence, successivement pour α, β , toutes les combinaisons que l'on peut former avec les nombres positifs moindres que 5, et pour γ les valeurs correspondantes également moindres que 5, données par la formule

$$\alpha + \beta \equiv H\gamma \pmod{5},$$

on trouve que la congruence $\alpha^5 + \beta^5 \equiv H\gamma^5 \pmod{25}$ ne peut subsister que lorsque γ est nul, on sera assuré que l'équation

$$x^5 \pm y^5 = 2^m \Lambda z^5$$

ne peut avoir lieu, à moins qu'on ne suppose z divisible par 5. On pourra donc, dans ce cas, mettre $5z$ à la place de z , ce qui change notre équation

en celle-ci :

$$x^5 \pm y^5 = 2^m 5^5 \Lambda z^5,$$

qui rentre évidemment dans le théorème II, et par conséquent est impossible. Or, ce cas a lieu toutes les fois que le nombre H est un des huit nombres suivans, 3, 4, 9, 12, 13, 16, 21, 22, comme on peut s'en assurer par un calcul très simple. Nous avons donc ainsi ce nouveau théorème :

Théorème III.

Les nombres m et Λ étant soumis aux mêmes restrictions que dans l'énoncé du théorème II, si le nombre $2^m \Lambda$, étant divisé par 25, donne un des huit restes suivans, 3, 4, 9, 12, 13, 16, 21, 22, il sera impossible de trouver deux nombres x et y premiers entre eux, tels que l'on ait $x^5 \pm y^5 = 2^m \Lambda z^5$.

Pour donner un exemple bien simple, considérons les deux équations suivantes: $x^5 \pm y^5 = 4z^5$, $x^5 \pm y^5 = 16z^5$.

Comme dans ces équations on peut, sans nuire à la généralité, supposer les nombres x et y premiers entre eux, il sera facile de voir qu'elles rentrent dans le théorème II. En effet, si l'on fait $\Lambda = 1$, et successivement $m = 2$, $m = 4$, on aura respectivement

$$2^m \Lambda = 4, \quad 2^m \Lambda = 16.$$

Il est donc prouvé que les deux équations précédentes sont impossibles.

Considérons encore l'équation

$$x^5 \pm y^5 = z^5,$$

qui est une de celles que Fermat a assurées être impossibles. Par des considérations semblables à celles qui nous ont servi pour établir le théorème précédent, on peut s'assurer que cette équation ne saurait subsister, à moins qu'une des indéterminées x , y , z , ne soit divisible par 5. Soit z l'indéterminée divisible par 5, car il est évident qu'on peut faire en sorte qu'une quelconque des indéterminées se trouve toute seule dans un membre. D'un autre côté, si l'on suppose ces indéterminées premières entre elles, l'une d'elles sera paire et les deux autres seront impaires. Si z était paire, on pourrait remplacer cette indéterminée par $2.5.z$, ce qui changerait l'équation précédente en celle-ci :

$$x^5 \pm y^5 = 2^4 5^5 z^5,$$

qui est impossible, puisqu'elle rentre évidemment dans le théorème II. Il ne resterait donc qu'à traiter le cas où l'indéterminée divisible par 5, serait impaire: mais la méthode exposée dans ce Mémoire paraît insuffisante pour ce cas, et je ne vois pas comment on pourrait compléter la démonstration du cas particulier du théorème de Fermat, dont il vient d'être question.

ADDITION AU MÉMOIRE PRÉCÉDENT.

(Cette Addition a été présentée à l'Académie, et paraphée par M. le secrétaire perpétuel Fourier, le 14 novembre 1825.)

Depuis que le Mémoire précédent a été présenté à l'Académie, M. Legendre a publié un second supplément à sa Théorie des nombres, dans lequel il démontre l'impossibilité de l'équation

$$x^5 \pm y^5 = z^5.$$

Le cas de l'indéterminée divisible en même temps par 2 et par 5, est traité dans cet ouvrage comme dans le Mémoire précédent, et l'auteur prouve ensuite l'impossibilité de l'autre cas au moyen d'une analyse nouvelle, quoique du même genre que celle qui sert pour le premier cas. L'objet de cette addition est d'établir deux théorèmes nouveaux sur les équations indéterminées du cinquième degré, et qui comprennent, comme cas particulier, le théorème de Fermat pour les cinquièmes puissances. Pour y parvenir, je m'appuie sur les résultats obtenus dans ce qui précède, et je fais usage d'une analyse semblable à celle dont M. Legendre s'est servi dans l'ouvrage cité, et que je présente de manière à montrer la grande analogie qu'elle a avec la méthode exposée dans le mémoire précédent.

Les nombres P et Q, dont le premier est supposé n'être pas divisible par 5, étant impairs tous les deux, et n'ayant pas de diviseur commun, le nombre $P^2 - 5Q^2$ sera de la forme $8k+4$, et l'on pourra faire

$$P^2 - 5Q^2 = 4L,$$

L étant un nombre impair et non-divisible par 5. Si nous multiplions membre par membre l'équation précédente et celle-ci.

$$3^2 - 5.1^2 = 4.$$

nous aurons

$$(3P \pm 5Q)^2 - 5(P \pm 3Q)^2 = 16L.$$

Comme les nombres P et Q sont impairs tous les deux, il est évident qu'en déterminant convenablement le signe, les expressions

$$\frac{3P \pm 5Q}{4} \quad \frac{P \pm 3Q}{4}$$

seront entières l'une et l'autre; faisant en conséquence

$$\frac{3P \pm 5Q}{4} = P', \quad \frac{\pm(P \pm 3Q)}{4} = Q',$$

le signe en dehors de la parenthèse étant choisi de manière à donner une valeur positive pour Q'. L'équation obtenue plus haut se changera en celle-ci. $P'^2 - 5Q'^2 = L$, et l'on s'assurera facilement que l'on a

$$P + Q\sqrt{5} = (P' \pm Q'\sqrt{5})(3 \pm \sqrt{5}).$$

les signes étant convenablement choisis, et que les nombres P' et Q' sont premiers entre eux, et de plus l'un pair, l'autre impair.

Supposons maintenant que le nombre L doive être une cinquième puissance. On satisfera à cette condition de la manière la plus générale en posant

$$P' + Q'\sqrt{5} = (M \pm N\sqrt{5})^5 (9 \pm 4\sqrt{5})^r.$$

En substituant cette valeur dans la dernière équation, on aura celle-ci:

$$P + Q\sqrt{5} = (M \pm N\sqrt{5})^5 (9 \pm 4\sqrt{5})^p (3 \pm \sqrt{5}).$$

dans laquelle les signes sont indépendans, comme dans les deux équations précédentes. On peut faire $p = 5k \pm r$, k étant entier et positif, et r ayant une de ces trois valeurs, 0, 1, 2, la quantité $(9 \pm 4\sqrt{5})^p$ se décomposera ainsi en ces deux facteurs $(9 \pm 4\sqrt{5})^{5k}$ et $(9 \pm 4\sqrt{5})^{\pm r}$ dont le premier peut être omis parce qu'il rentre dans $(M \pm N\sqrt{5})^5$. Si nous observons de plus qu'en vertu de l'équation

$$9 \pm 4\sqrt{5} = (9 \mp 4\sqrt{5})^{-1},$$

on peut changer dans $(9 \pm 4\sqrt{5})^{\pm r}$ simultanément les signes de r et du radical, nous pouvons supposer le signe de r positif, et l'équation donnée plus haut deviendra

$$P + Q\sqrt{5} = (M \pm N\sqrt{5})^3 (9 \pm 4\sqrt{5})^r (3 \pm \sqrt{5}).$$

L devant toujours être la cinquième puissance d'un nombre impair et non-divisible par 5, déterminons les conditions nécessaires pour que Q soit divisible par 5. Comme le coefficient de $\sqrt{5}$, dans le développement de $(M \pm N\sqrt{5})^5$ est divisible par 5, et que la partie rationnelle de ce développement ne l'est pas, M n'étant pas divisible par 5, on conclut, comme dans la démonstration du théorème I, que pour que Q puisse être divisible par 5, il faut que le coefficient de $\sqrt{5}$, dans la valeur développée de $(9 \pm 4\sqrt{5})^r (3 \pm \sqrt{5})$ le soit.

Or, en substituant pour r successivement les trois valeurs 0, 1, 2, on trouve que cela n'a lieu que dans le cas de $r = 2$, les signes des radicaux dans les deux facteurs $(9 \pm 4\sqrt{5})^r$ et $(3 \pm \sqrt{5})$ étant en même temps opposés. Si l'on fait attention que l'on a

$$\frac{(3 \pm \sqrt{5})^3}{2^3} = 9 \pm 4\sqrt{5} \quad \text{et} \quad 3 \mp \sqrt{5} = \frac{4}{3 \pm \sqrt{5}},$$

on trouvera que le produit précédent sera, dans le cas dont il s'agit, équivalent à

$$\frac{(3 \pm \sqrt{5})^3}{2^4}.$$

valeur dont la substitution dans l'équation obtenue plus haut, la change en celle-ci:

$$P + Q\sqrt{5} = \frac{(M \pm N\sqrt{5})^3 (3 \pm \sqrt{5})^3}{2^4}.$$

Les nombres M et N étant l'un pair, l'autre impair, les nombres φ et ψ déterminés par l'équation

$$\varphi + \psi\sqrt{5} = (M \pm N\sqrt{5})(3 \pm \sqrt{5})$$

seront impairs l'un et l'autre, et l'on aura

$$P + Q\sqrt{5} = \frac{(\varphi + \psi\sqrt{5})^3}{2^4}$$

et par conséquent

$$P = g \frac{(g^4 + 2 \cdot 5^2 g^2 \psi^2 + 5^3 \psi^4)}{2^4},$$

$$Q = 5\psi \frac{(g^4 + 10g^2\psi^2 + 5\psi^4)}{2^4}.$$

Pour que P et Q soient premiers entre eux, il faut que g et ψ n'aient pas de diviseur commun, et que le premier de ces nombres ne soit pas divisible par 5, et réciproquement, si les nombres g et ψ , dont le premier est supposé ne pas être divisible par 5, n'ont pas de diviseur commun, et sont impairs l'un et l'autre, les nombres P et Q seront entiers et premiers entre eux. En effet, le quart de la quantité $g^4 + 10g^2\psi^2 + 5\psi^4$, pouvant se mettre sous la forme

$$\left(\frac{g^2 + 5\psi^2}{2}\right)^2 - 5(\psi^2)^2,$$

et cette dernière expression étant évidemment le quadruple d'un nombre impair, on voit que la valeur de Q est entière et impaire; la même chose se prouvera pour la valeur de P, et l'on s'assurera facilement que les nombres P et Q, qui sont impairs tous les deux, n'ont pas de diviseur commun. Nous avons donc ainsi ce théorème:

Théorème IV.

„Les nombres P et Q devant être premiers entre eux, et impairs l'un et l'autre, et le dernier devant être divisible par 5, je dis que pour égaliser le „binôme $P^2 - 5Q^2$, au quadruple d'une cinquième puissance avec toute la „ralité convenable, il suffira de poser

$$P + Q\sqrt{5} = \frac{(g + \psi\sqrt{5})^5}{2^4},$$

„les nombres indéterminés g et ψ étant premiers entre eux, impairs l'un et l'autre, et le premier de plus non-divisible par 5 (*).”

Voici maintenant le premier des théorèmes nouveaux que nous avons annoncés au commencement de cette addition.

(*) Ce théorème, comme le théorème I, a ses analogues pour beaucoup d'autres nombres premiers.

Théorème V.

„La lettre n désignant un nombre positif autre que 0 et 2, et le nombre A n'étant divisible ni par 2 ni par 5, ni par aucun nombre premier de l'une de ces deux formes $10k \pm 1$, il sera impossible de trouver deux nombres x et y premiers entre eux, et tels que

$$x^5 \pm y^5 = 5^n A z^5 \quad (y)."$$

Les nombres x et y peuvent être impairs tous les deux, ou l'un pair et l'autre impair. Dans le premier cas, z sera divisible par 2, et l'on pourra mettre $2z$ à la place de z , ce qui changera l'équation (y) en celle-ci :

$$x^5 \pm y^5 = 2^5 5^n A z^5,$$

qui est impossible puisqu'elle rentre évidemment dans le théorème II. Reste donc à prouver l'impossibilité du second cas où l'on suppose les nombres x, y , l'un pair, l'autre impair. Si nous faisons

$$x \pm y = p, \quad x \mp y = q,$$

nous aurons

$$2x = p + q, \quad \pm 2y = p - q,$$

et les nombres p et q seront premiers entre eux, et de plus impairs l'un et l'autre. En substituant les valeurs précédentes de $2x$ et $\pm 2y$ dans l'équation (y), après en avoir multiplié les deux membres par 2^5 , on aura

$$p(p^4 + 10p^2q^2 + 5q^4) = 2^4 5^n A z^5.$$

Comme p doit évidemment être divisible par 5, nous ferons $p = 5r$, ce qui donnera

$$5^2 r(q^4 + 2 \cdot 5^2 q^2 r^2 + 5^3 r^4) = 2^4 5^n A z^5.$$

Le nombre n est par hypothèse égal à l'unité ou plus grand que 2. Si n est égal à l'unité, il faudra, dans l'équation précédente, supposer z divisible par 5. On pourra donc, dans ce cas, mettre $5z$ à la place de z , ou, ce qui est la même chose, donner à 5 l'exposant 6, d'où l'on voit que l'on peut supposer dans tous les cas que $n > 2$.

Si l'on met l'équation précédente sous cette forme

$$r(q^4 + 2 \cdot 5^2 q^2 r^2 + 5^3 r^4) = 2^4 5^{n-2} A z^5,$$

et qu'on fasse attention que $n > 2$, et que q est premier à $p = 5r$, on voit que r doit être supposé divisible par 5.

Choisissons maintenant un nombre positif ν tel que $n+\nu-2$ soit divisible par 5 et un nombre B qui n'ait d'autre diviseur premier que le nombre A et tel que le produit AB soit une cinquième puissance. Multipliant la dernière équation par $5^\nu B$, nous aurons

$$5^\nu B r (q^4 + 2 \cdot 5^2 q^2 r^2 + 5^3 r^4) = 2^4 5^{n+\nu-2} A B z^5.$$

Le facteur trinome pouvant se mettre sous la forme $(q^2 + 5^2 r^2)^2 - 5(10r^2)^2$ et les nombres $q^2 + 5^2 r^2$, $10r^2$ n'ayant évidemment d'autre diviseur commun que 2, tous les diviseurs premiers impairs du facteur trinome seront d'une de ces formes $10k \pm 1$, et le facteur trinome sera par conséquent premier à B. Il est évident qu'il est aussi premier à $5^\nu r$, et par conséquent à $5^\nu B r$.

Comme le facteur $5^\nu B r$ et le facteur trinome sont premiers entre eux, et que le premier de ces facteurs est impair, il faut en vertu de la dernière équation, dont le second membre est le produit de 2^4 et de la cinquième puissance d'un nombre impair, que $5^\nu B r$ soit une cinquième puissance, et le facteur trinome une cinquième puissance multipliée par 2^4 .

Le quart du facteur trinome devant être le quadruple d'une cinquième puissance, et ce quart pouvant se mettre sous la forme

$$\left(\frac{q^2 + 5^2 r^2}{2} \right)^2 - 5(5r^2)^2,$$

où les nombres $\frac{q^2 + 5^2 r^2}{2}$, $5r^2$, sont évidemment premiers entre eux, impairs l'un et l'autre, et le dernier de plus divisible par 5, il suffira en vertu du théorème établi au commencement de cette addition, pour égaler le quart du facteur trinome au quadruple d'une cinquième puissance, de poser ces deux équations

$$\begin{aligned} \frac{q^2 + 5^2 r^2}{2} &= t \frac{(t^4 + 2 \cdot 5^2 t^2 s^2 + 5^3 s^4)}{2^4} \\ 5r^2 &= 5s \frac{(t^4 + 10t^2 s^2 + 5s^4)}{2^4}, \end{aligned}$$

les nombres indéterminés t et s devant être supposés premiers entre eux, impairs l'un et l'autre, et le premier de plus non-divisible par 5. Comme t n'est pas divisible par 5, et que ν l'est comme nous l'avons vu ci-dessus, il faut, en vertu de la dernière des équations précédentes, que s soit divisible par 5.

Nous avons vu plus haut que $5^r B^r$ devait être une cinquième puissance. Le nombre $5^{2r} B^2 r^2$, carré du précédent, devra donc être une puissance du même degré, et même du dixième degré.

Or, en multipliant par $2^4 5^{2r-1} B^2$ les deux membres de la dernière équation, on aura celle-ci :

$$2^4 5^{2r} B^2 r^2 = 5^{2r} B^2 s(t^4 + 10t^2 s^2 + 5s^4).$$

Si donc nous faisons pour abrégér $2r = h$, $B^2 = C$, tout se réduit à faire voir qu'il est impossible de trouver deux nombres t et s premiers entre eux, impairs l'un et l'autre, et dont le dernier s soit de plus divisible par 5, tels que le produit

$$5^h C s(t^4 + 10t^2 s^2 + 5s^4) \quad (d)$$

soit une cinquième puissance multipliée par 2^4 .

Il est facile de voir que le produit (d) ne saurait être le produit de 2^4 et d'une cinquième puissance, à moins que $5^h C s$ ne soit une cinquième puissance, et le facteur trinôme une cinquième puissance multipliée par 2^4 .

Le quart du facteur trinôme devant être le quadruple d'une cinquième puissance, et ce quart pouvant se mettre sous la forme

$$\left(\frac{t^2 + 5s^2}{2}\right)^2 - 5(s^2)^2.$$

où les nombres $\frac{t^2 + 5s^2}{2}$, s^2 sont évidemment premiers entre eux, impairs l'un et l'autre, et le dernier de plus divisible par 5, il suffira, pour égaler le facteur trinôme divisé par 4 au quadruple d'une cinquième puissance, de poser ces équations

$$\frac{t^2 + 5s^2}{2} = t' \frac{(t'^4 + 2 \cdot 5^2 t'^2 s'^2 + 5^3 s'^4)}{2^4}$$

$$s^2 = 5s' \frac{(t'^4 + 10t'^2 s'^2 + 5s'^4)}{2^4},$$

les nombres t' et s' étant supposés premiers entre eux, impairs l'un et l'autre, et le premier t' de plus non-divisible par 5. Comme s est divisible par 5, et que t' ne l'est plus, il faut, d'après la dernière équation, que s' soit aussi divisible par 5. On conclut encore de la dernière équation, que $\frac{25}{16} s'^5 < s^2$ et par suite que s' est beaucoup plus petit que s .

Le nombre $5^h C s$ devant être une cinquième puissance, $5^{2h} C^2 s^2$ carré du nombre précédent, devra être une puissance du même degré, et même du dixième

degré. Or, en multipliant par $2^4 5^{2h} C^2$ les deux membres de la dernière équation, on aura celle-ci :

$$2^4 5^{2h} C^2 s'^2 = 5^{2h+1} C'^2 s' (t'^4 + 10 t'^2 s'^2 + 5 s'^4)$$

ou ce qui est la même chose, en faisant $2h+1 = h'$, $C^2 = C'$, dans le second membre.

$$2^4 5^{2h} C^2 s'^2 = 5^{h'} C' s' (t'^4 + 10 t'^2 s'^2 + 5 s'^4). \quad (\delta')$$

équation dont les deux membres devront être des cinquièmes puissances multipliées par 2^4 .

Le produit (δ') étant parfaitement semblable au produit (δ) , et le nombre s' étant beaucoup plus petit que le nombre s , on conclura, comme dans la démonstration du théorème II du mémoire précédent, que le produit (δ) ne saurait être égal à une cinquième puissance, multipliée par 2^4 , et que par conséquent l'équation (γ) ne saurait avoir lieu.

Le théorème de Fermat, pour le cas des cinquièmes puissances, est compris comme cas particulier dans le théorème que nous venons d'établir. En effet, l'équation $x^5 \pm y^5 = z^5$ ne pouvant avoir lieu, à moins qu'une des indéterminées, z par exemple, ne soit divisible par 5, nous pouvons mettre $5z$ à la place de z ; ce qui donnera $x^5 \pm y^5 = 5^5 z^5$, équation impossible, puisqu'elle rentre dans le dernier théorème.

Un raisonnement tout-à-fait semblable à celui au moyen duquel nous avons établi le théorème III, en partant du théorème II, peut servir à déduire du théorème que nous venons de démontrer un nouveau théorème qui peut s'énoncer comme il suit :

Théorème VI.

Le nombre A étant soumis aux mêmes restrictions que dans l'énoncé du théorème V, et ce nombre donnant un des huit restes suivants, 3, 4, 9, 12, 13, 16, 21, 22, lorsqu'il est divisé par 25, il sera impossible de trouver deux nombres x et y premiers entre eux, et tels que l'on ait $x^5 \pm y^5 = A z^5$.

FIN.

MÉMOIRE SUR L'IMPOSSIBILITÉ DE QUELQUES
ÉQUATIONS INDÉTERMINÉES DU CINQUIÈME
DEGRÉ.

PAR

Mr. LEJEUNE DIRICHLET,
PROFESSEUR EN MATHÉMATIQUES.

LU A L'ACADÉMIE ROYALE DES SCIENCES (INSTITUT DE FRANCE), LE 11 JUILLET 1825,
PAR L'AUTEUR.

Crelle. Journal für die reine und angewandte Mathematik, Bd. 3 S. 354—375.

MÉMOIRE SUR L'IMPOSSIBILITÉ DE QUELQUES ÉQUATIONS INDÉTERMINÉES DU CINQUIÈME DEGRÉ.

Lu à l'Académie royale des Sciences (Institut de France) le 11 juillet 1825, par l'auteur.

(D'APRÈS LE RAPPORT DE MM. LACROIX ET LEGENDRE, CE MÉMOIRE A ÉTÉ APPROUVÉ, ET
DOIT ÊTRE IMPRIMÉ DANS LE RECUEIL DES MÉMOIRES DE SAVANTS ÉTRANGERS*).

On sait que la théorie des équations indéterminées des degrés supérieurs au second, est encore très peu avancée; il est vrai qu'il y a une infinité d'équations de tous les degrés dont on peut démontrer l'impossibilité en faisant voir que quelles que soient les valeurs que l'on attribue aux indéterminées, les deux membres de l'équation proposée ne peuvent le même reste lorsqu'on les divise par un certain nombre ou module; mais lorsqu'une équation ne peut pas être traitée par ce moyen, il devient difficile de prouver qu'elle est impossible, et on n'y est parvenu, jusqu'à présent, que pour un très petit nombre d'équations. Toutes ces équations sont très particulières, et d'une forme telle, que lorsqu'on cherche à les résoudre, on est naturellement conduit à une ou plusieurs formules quadratiques qu'il s'agit d'égaliser à des puissances parfaites. On satisfait ensuite de la manière la plus générale à cette condition, en exprimant les indéterminées par d'autres, dont les premières deviennent des fonctions entières, et il se trouve, du moins dans tous les cas où la méthode dont il est question réussit, que les nouvelles indéterminées ou d'autres quantités qui en dépendent d'une manière très simple, satisfont également à une équation semblable à l'équation proposée. Comme les nouvelles indéterminées sont en même temps plus petites que les indéterminées primitives, l'impossibilité de l'équation proposée se trouve établie; car il est évident que si elle était possible, on aurait le moyen d'obtenir une suite décroissante et indéfinie de nombres entiers, ce qui implique contradiction. C'est de cette

* Ce Mémoire n'a pas encore été publié jusqu'ici.

(Note d. réd.)

manière que FERMAT et EULER ont prouvé l'impossibilité de plusieurs équations du troisième et du quatrième degré.

En essayant d'appliquer des considérations semblables à quelques équations du cinquième degré et d'une forme analogue à celles des équations traitées par FERMAT et EULER, on est arrêté tout aussitôt. La formule quadratique à laquelle on arrive, et qu'il faut égaler à une cinquième puissance, admet plusieurs solutions différentes, et parmi ces solutions, il n'y en a qu'une seule qui conduise à une équation semblable à l'équation proposée. En réfléchissant à cette difficulté, j'ai reconnu qu'elle pouvait être levée très simplement en assujettissant à quelques conditions le nombre déterminé qui entre dans l'équation. Il résulte d'un théorème exposé dans les préliminaires, que lorsque ces conditions se trouvent remplies, les différentes solutions dont la formule quadratique est susceptible, en général, doivent être rejetées, à l'exception d'une seule, qui est précisément celle de laquelle on déduit des nombres qui satisfont à une équation semblable à l'équation proposée. On parvient ainsi à établir l'impossibilité d'une classe assez étendue d'équations indéterminées du cinquième degré. Le premier membre de ces équations est la somme ou la différence de deux cinquièmes puissances, et le second membre est le produit d'une cinquième puissance et d'un nombre déterminé assujetti à différentes conditions. En attribuant à ce nombre des valeurs particulières compatibles avec ces conditions, on peut obtenir autant de théorèmes particuliers que l'on veut. Cette généralité de nos théorèmes est d'autant plus singulière, que les équations analogues du troisième et du quatrième degré, dont l'impossibilité a été démontrée jusqu'à présent, ne sont qu'en nombre fini et même très petit.

Théorème I.

Soit l un nombre premier impair non-diviseur du nombre a et supposons que l'on ait :

$$(1) \quad d^2 - a\varepsilon^2 = l;$$

ou satisfera, comme on sait, à l'équation :

$$(2) \quad d^2 - ac^2 = l^n$$

par les nombres d et c que donne la formule :

$$(3) \quad (d + \varepsilon \sqrt{a})^n = d + c\sqrt{a},$$

lorsqu'on y égale les parties rationnelles et les coefficients de \sqrt{a} : je dis de plus que les nombres d et e ainsi obtenus seront premiers entre eux^{*)}.

Il est évident, par l'équation (2), que si les nombres d et e avaient un diviseur commun, ce ne pourrait être que le nombre l ou une puissance de ce nombre. Il suffira donc de faire voir que d n'est pas divisible par l . La formule (3) donne cette valeur de d :

$$d = \delta^n + \frac{n(n-1)}{1 \cdot 2} a \delta^{n-2} \varepsilon^2 + \frac{n(n-1)(n-2)(n-3)}{1 \cdot 2 \cdot 3 \cdot 4} a^2 \delta^{n-4} \varepsilon^4 + \text{etc.}$$

D'un autre côté, on conclut de l'équation (1), en se servant du signe employé par M. GAUSS:

$$\delta^2 \equiv a \varepsilon^2, \quad \delta^4 \equiv a^2 \varepsilon^4, \quad \delta^6 \equiv a^3 \varepsilon^6, \quad \dots \pmod{l},$$

et en multipliant respectivement par δ^{n-2} , δ^{n-4} , ...:

$$\delta^n \equiv a \delta^{n-2} \varepsilon^2, \quad \delta^n \equiv a^2 \delta^{n-4} \varepsilon^4, \quad \dots \pmod{l}.$$

En combinant ces congruences avec l'équation qui donne d , on aura:

$$d \equiv \delta^n \left(1 + \frac{n(n-1)}{1 \cdot 2} + \frac{n(n-1)(n-2)(n-3)}{1 \cdot 2 \cdot 3 \cdot 4} + \text{etc.} \right),$$

ou, ce qui est la même chose, la quantité entre les crochets étant le développement de $\frac{1}{2}[(1+1)^n + (1-1)^n]$ et par conséquent égale à 2^{n-1} :

$$d \equiv 2^{n-1} \delta^n \pmod{l}.$$

Il est maintenant facile de voir que d n'est pas divisible par l , car il faudrait pour cela que δ fût divisible par l ; mais la seule inspection de l'équation (1) montre que cela est impossible. δ et ε étant évidemment premiers entre eux et a non divisible par l .

Théorème II.

„La lettre l désignant un nombre premier impair non-diviseur de a , si l'on suppose que l'on ait:

$$(4) \quad d^2 - a e^2 = l^n,$$

$$(5) \quad d'^2 - a e'^2 = l^n,$$

les nombres d et e , d' et e' étant premiers entre eux, je dis que l'on pourra

^{*)} Si le nombre l , au lieu d'être premier, était un nombre impair quelconque et que les nombres δ et a fussent premiers entre eux, les nombres d et $a e$ seraient également premiers entre eux, comme il est facile de s'en assurer par un raisonnement parfaitement semblable à celui dont nous faisons usage dans le texte.

trouver deux nombres t et u satisfaisant à l'équation:

$$(6) \quad t^2 - au^2 = 1$$

et en outre tels que l'on ait:

$$(7) \quad (d' \pm e' \sqrt{a})(t \pm u \sqrt{a}) = d + e \sqrt{a},$$

les signes étant convenablement choisis et les parties rationnelles et les coefficients de \sqrt{a} égaux séparément.*

Les équations (4) et (5) donnent immédiatement:

$$d^2 \equiv ae^2, \quad d'^2 \equiv ae'^2, \quad (\text{mod. } l^n);$$

on conclut de là en multipliant membre à membre:

$$d^2 d'^2 \equiv a^2 e^2 e'^2 \quad (\text{mod. } l^n),$$

et en transposant:

$$d^2 d'^2 - a^2 e^2 e'^2 \equiv (dd' + ace')(dd' - ace') \equiv 0 \quad (\text{mod. } l^n).$$

On voit par cette congruence qu'un des nombres $dd' + ace'$, $dd' - ace'$ est divisible par l^n ou qu'ils sont l'un et l'autre divisibles par l^n .

Mais il est facile de voir que ce dernier cas est impossible; en effet, si ces nombres étaient tous les deux divisibles par l , leur somme $2dd'$ le serait également; il faudrait donc, dans ce cas, qu'un des nombres d , d' fût divisible par l ; mais on s'assurera facilement que cela ne saurait être, en ayant égard aux suppositions faites dans l'énoncé du théorème. L'expression $\frac{dd' \pm ace'}{l^n}$ avec le signe convenable sera donc un entier. Nous ferons, pour plus de simplicité, $i = \pm 1$, i étant choisi de manière à rendre entière l'expression précédente.

Si l'on multiplie membre à membre les équations (4) et (5), on aura celle-ci:

$$(dd' \pm ace')^2 - a(d' \pm de')^2 = e^{2n},$$

dans laquelle on peut prendre à volonté les signes supérieurs ou les signes inférieurs. On a donc aussi:

$$(dd' + iace')^2 - a(d'e + ide')^2 = l^{2n}.$$

Le nombre $dd' + iace'$ étant divisible par l^n , et a n'étant pas divisible par l ,

* Dans le cas de $n = 1$, la première hypothèse est comprise dans la seconde et a par conséquent nécessairement lieu, mais le même raisonnement prouverait toujours l'impossibilité de la seconde.

ou voit, par l'équation précédente que $d'e + ide'$ est également divisible par l^n . Cela posé, je dis qu'on aura :

$$t = \frac{dd' + iace'}{l^n}, \quad u = \frac{i'(d'e + ide')}{l^n},$$

i' étant 1, ou -1 selon que la quantité entre les parenthèses est positive ou négative. En effet, on aura en divisant les deux nombres de l'équation donnée plus haut par l^{2n} :

$$\left(\frac{dd' + iace'}{l^n}\right)^2 - a\left(\frac{d'e + ide'}{l^n}\right)^2 = 1,$$

ou, ce qui est la même chose, $t^2 - au^2 = 1$, et on s'assurera facilement par la substitution que les valeurs précédentes de t et u satisfont aussi à l'équation (7), en y déterminant les signes de cette manière :

$$(d' - ie'\sqrt{a})(t + i'u\sqrt{a}) = d + e\sqrt{a}.$$

Remarque. Comme il est évident qu'on peut changer simultanément les signes de e' , u , e dans l'équation :

$$(d' \pm e'\sqrt{a})(t \pm u\sqrt{a}) = d + e\sqrt{a},$$

on voit que l'on peut poser :

$$(d' \pm e'\sqrt{a})(t \pm u\sqrt{a}) = (d \pm e\sqrt{a}),$$

le signe de e étant à volonté et les signes de e' et u étant convenablement choisis.

Théorème III.

„La lettre l désignant un nombre premier impair non-diviseur de a , et k un nombre impair qui n'a pas de diviseur commun avec a et qui n'est pas divisible par l , si nous supposons que l'on ait ces deux équations $D^2 - aE^2 = l^2k$, $d^2 - ae^2 = l^n$, et que les nombres D et E , d et e soient premiers entre eux, je dis que l'on pourra trouver deux nombres D' et E' , premiers entre eux, satisfaisant à l'équation $D'^2 - aE'^2 = k$, et en outre tels que l'on ait :

$$(D' \pm E'\sqrt{a})(d \pm e\sqrt{a}) = D + E\sqrt{a},$$

les signes étant convenablement choisis et les parties rationnelles et les coefficients de \sqrt{a} étant égaux séparément.

La démonstration de ce théorème est tellement semblable à celle du théorème II. que nous nous dispenserons de la développer ici.

Il y a ici une remarque semblable à faire et l'on voit très facilement que l'on peut poser:

$$(D' \pm E' \sqrt{a})(d \pm e \sqrt{a}) = D \pm E \sqrt{a},$$

le signe de E étant à volonté et les signes de E' et e étant convenablement choisis.

Les théorèmes que nous venons d'établir et qui peuvent être utiles dans plusieurs occasions, vont nous servir maintenant à établir une proposition relative à la manière de rendre le binôme $P^2 - 5Q^2$, dans lequel P et Q sont des nombres indéterminés soumis à la restriction d'être premiers entre eux, égal à une cinquième puissance. Cette proposition consiste en ce que, pour égaliser le binôme $P^2 - 5Q^2$ de la manière la plus générale à une cinquième puissance impaire et non-divisible par 5, on n'a qu'à poser:

$$P + Q\sqrt{5} = (M \pm N\sqrt{5})^5 (t \pm u\sqrt{5}),$$

M et N étant de nouvelles indéterminées soumises à la seule restriction d'être premières entre elles, l'une paire, l'autre impaire et la première de plus non-divisible par 5; et les lettres t et u désignant la solution générale de l'équation $t^2 - 5u^2 = 1$; ce qui veut dire que toutes les fois que, P et Q étant premiers entre eux, le binôme $P^2 - 5Q^2$ est une cinquième puissance impaire non-divisible par 5, il existe des nombres M et N premiers entre eux et tels qu'on ait:

$$P + Q\sqrt{5} = (M \pm N\sqrt{5})^5 (t \pm u\sqrt{5}),$$

t et u satisfaisant à l'équation $t^2 - 5u^2 = 1$.

Pour nous assurer de la vérité de cette proposition, posons $P^2 - 5Q^2 = L$, L désignant une cinquième puissance impaire, non-divisible par 5 et voyons ce qui en résulte sur la nature des nombres P et Q . Désignons par l l'un quelconque des diviseurs premiers de L et soit l^{5m} la puissance la plus élevée de l , qui divise L , de sorte qu'en faisant $L = l^{5m} L'$, L' soit premier à l . Il résulte d'un théorème connu, que le nombre l qui divise $P^2 - 5Q^2$ sera lui-même de la forme $\delta^2 - 5\epsilon^2$. Si nous posons maintenant:

$$(\delta + \epsilon\sqrt{5})^n = d + e\sqrt{5}, \quad (\delta + \epsilon\sqrt{5})^{5n} = D + E\sqrt{5},$$

d et e , D et E seront premiers entre eux en vertu du théorème I., et l'on aura l'équation:

$$(d + e\sqrt{5})^5 = D + E\sqrt{5}.$$

Si l'on applique ensuite le théorème III. aux équations:

$$D^2 - 5E^2 = l^{5n}, \quad P^2 - 5Q^2 = l^{5n} L',$$

qui se déduisent immédiatement de ce qui précède, on verra qu'il existe des nombres P' et Q' , premiers entre eux et tels qu'on ait:

$$P'^2 - 5Q'^2 = L', \quad P' + Q'\sqrt{5} = (D \pm E\sqrt{5})(P' \pm Q'\sqrt{5}),$$

ou, ce qui revient au même, en remplaçant $D + E\sqrt{5}$ par $(d + e\sqrt{5})^5$:

$$P' + Q'\sqrt{5} = (d \pm e\sqrt{5})^5 (P' \pm Q'\sqrt{5}).$$

L'équation $P'^2 - 5Q'^2 = L'$ à laquelle nous venons de parvenir, est entièrement analogue à l'équation $P^2 - 5Q^2 = L$, car le nombre L' que l'on obtient en divisant L par l^{5n} est une cinquième puissance, comme L . Supposons pour un instant que la proposition que nous cherchons à démontrer soit vraie pour l'équation $P'^2 - 5Q'^2 = L'$, et voyons comment on pourrait en conclure qu'elle a également lieu pour le binôme $P^2 - 5Q^2$. Dans la supposition que nous venons de faire, il existe des nombres M' et N' tels qu'on ait:

$$P' + Q'\sqrt{5} = (M' \pm N'\sqrt{5})^5 (t \pm u\sqrt{5}).$$

En mettant cette valeur de $P' + Q'\sqrt{5}$ dans l'équation obtenue plus haut et dont le premier membre renferme $P + Q\sqrt{5}$, il viendra celle-ci:

$$P + Q\sqrt{5} = (M' \pm N'\sqrt{5})^5 (d \pm e\sqrt{5})^5 (t \pm u\sqrt{5}),$$

dans laquelle les signes dépendent de ceux qui se trouvent dans les deux équations dont la combinaison l'a produite. Si nous posons maintenant:

$$(M' \pm N'\sqrt{5})(d \pm e\sqrt{5}) = M \pm N\sqrt{5}.$$

le signe de N étant $+$ ou $-$, selon que le coefficient de $\sqrt{5}$, dans la valeur développée du premier membre, est positif ou négatif, l'équation précédente se changera en celle-ci:

$$P + Q\sqrt{5} = (M \pm N\sqrt{5})^5 (t \pm u\sqrt{5}),$$

qui est conforme à l'énoncé de la proposition dont nous nous occupons.

Ayant ainsi fait voir que la proposition en question est vraie pour le binôme $P^2 - 5Q^2$ égal à la cinquième puissance L , si elle est supposée avoir lieu pour le binôme $P^2 - 5Q^2$, égal à la cinquième puissance L' , qui a un diviseur premier de moins que L , il ne reste, pour rendre la démonstration

complète, qu'à prouver la vérité de notre proposition pour le cas où le binôme $P^2 - 5Q^2$ est une cinquième puissance qui n'a qu'un seul diviseur premier l . Or, c'est ce qu'il est très facile de faire en s'appuyant sur le théorème II. En effet, dans le cas que nous venons d'énoncer, on a $P^2 - 5Q^2 = l^{5n}$; d'un autre côté, le nombre l pouvant être mis sous la forme $\delta^2 - 5\epsilon^2$, si l'on fait:

$$(\delta + \epsilon\sqrt{5})^n = M + N\sqrt{5}, \quad (\delta + \epsilon\sqrt{5})^{5n} = D + E\sqrt{5},$$

on aura aussi:

$$D + E\sqrt{5} = (M + N\sqrt{5})^5. \quad D^2 - 5E^2 = l^{5n}.$$

D et E étant premiers entre eux en vertu du théorème I. Cela posé, il résulte immédiatement de l'application du théorème II. aux équations:

$$P^2 - 5Q^2 = l^{5n}, \quad D^2 - 5E^2 = l^{5n},$$

qu'on a la relation:

$$P + Q\sqrt{5} = (D \pm E\sqrt{5})(t \pm u\sqrt{5}),$$

t et u satisfaisant à l'équation $t^2 - 5u^2 = 1$ et les signes étant convenablement choisis; ou, ce qui revient au même, en mettant $(M \pm N\sqrt{5})^5$ à la place de $D \pm E\sqrt{5}$:

$$P + Q\sqrt{5} = (M \pm N\sqrt{5})^5 (t \pm u\sqrt{5}).$$

résultat conforme à l'énoncé de notre proposition. Il est ainsi prouvé que toutes les fois que $P^2 - 5Q^2$ est une cinquième puissance impaire, il existe des nombres M et N qui satisfont à la formule précédente. Quant à l'inverse de cette proposition, savoir qu'en attribuant dans la formule précédente à M et N des valeurs soumises aux seules restrictions déjà plusieurs fois énoncées, on obtiendra des nombres P et Q premiers entre eux et tels que $P^2 - 5Q^2$ soit une cinquième puissance, la démonstration en est tellement simple qu'il est inutile de nous y arrêter. — Au moyen de ce qui précède il sera facile d'établir le théorème que nous allons énoncer et qui servira de base aux propositions qui font l'objet principal de ce mémoire.

Théorème IV.

«Les nombres P et Q devant être premiers entre eux, l'un pair, l'autre impair, et le dernier devant être de plus divisible par 5, je dis que pour égaliser le binôme $P^2 - 5Q^2$ de la manière la plus générale à une cinquième

puissance, il suffira de poser:

$$P+Q\sqrt{5} = (g+\psi\sqrt{5})^5.$$

Les indéterminées g et ψ étant premières entre elles, l'une paire, l'autre impaire, et la première de plus non-divisible par 5*).

Pour égaler P^2-5Q^2 à une cinquième puissance, nous poserons, d'après ce qui vient d'être dit:

$$P+Q\sqrt{5} = (M\pm N\sqrt{5})(t\pm u\sqrt{5}).$$

Le nombre M n'étant pas divisible par 5, si nous faisons pour un instant:

$$(M+N\sqrt{5})^5 = M'+N'\sqrt{5},$$

il sera facile de voir que N' est divisible par 5, et que M' ne l'est pas. En substituant l'expression précédente dans la valeur de $P+Q\sqrt{5}$, on aura:

$$P+Q\sqrt{5} = (M'\pm N'\sqrt{5})(t\pm u\sqrt{5}),$$

d'où l'on tire:

$$Q = \pm M'u \pm N't.$$

N' étant divisible par 5, et M' ne l'étant pas, il est évident que Q ne pourra être divisible par 5, qu'autant que u le sera. Les valeurs les plus petites qui satisfassent à l'équation:

$$t^2-5u^2 = 1,$$

sont celles-ci:

$$t = 9, \quad u = 4.$$

Les valeurs générales seront par conséquent données par cette formule:

$$t+u\sqrt{5} = (9+4\sqrt{5})^p,$$

dans laquelle p est un nombre entier, positif quelconque**); on tire de là

$$u = \frac{p}{1} 9^{p-1} \cdot 4 + \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3} 9^{p-3} \cdot 4^3 \cdot 5 + \text{etc.}$$

Tous les termes, à partir du second, étant divisibles par 5, quel que soit p , on voit que pour que u puisse être divisible par 5, il faut que le premier terme, et par conséquent aussi p , soit divisible par 5. Si nous faisons donc $p = 5p'$, p' étant un entier, et que nous substituions la

* Il n'est peut-être pas inutile de faire remarquer qu'il y a des théorèmes analogues pour beaucoup d'autres nombres premiers, et que pour les établir, on peut faire usage des mêmes considérations dont nous nous servons ici.

***) Voyez les Additions à l'Algèbre d'EULER (art. 75).

valeur de $t + u\sqrt{5}$ dans celle de $P + Q\sqrt{5}$, nous aurons :

$$P + Q\sqrt{5} = (M \pm N\sqrt{5})^5 (9 \pm 4\sqrt{5})^{5p'}$$

résultat qui, par l'introduction des nouvelles indéterminées g et ψ telles que l'on ait :

$$(M \pm N\sqrt{5})(9 \pm 4\sqrt{5})^{p'} = g + \psi\sqrt{5}$$

se change en celui-ci :

$$P + Q\sqrt{5} = (g + \psi\sqrt{5})^5$$

La forme de la solution donnée par l'énoncé du théorème se trouvant ainsi justifiée, il ne reste plus qu'à déterminer la nature des indéterminées.

Comme on a :

$$P^2 - 5Q^2 = (g^2 - 5\psi^2)^5,$$

et que les nombres P et Q sont respectivement divisibles par g et ψ , on voit facilement que les indéterminées g et ψ doivent être supposées premières entre elles, l'une paire, l'autre impaire, et la première de plus non-divisible par 5. On peut même ajouter que g ou ψ sera impaire selon que P ou Q l'est. Réciproquement, si les indéterminées g et ψ satisfont aux conditions précédentes, les nombres P et Q déterminés par la formule :

$$P + Q\sqrt{5} = (g + \psi\sqrt{5})^5,$$

seront premiers entre eux, comme il est facile de s'en assurer. Ces préliminaires établis, nous pourrions nous occuper des théorèmes qui font l'objet principal de ce Mémoire. Le premier de ces théorèmes peut s'énoncer de la manière suivante.

Théorème V.

Les nombres m et n étant positifs, plus grands que zéro, le second de plus différent de 2, et le nombre A n'étant divisible ni par 2 ni par 5, ni par aucun nombre premier de la forme $10k+1$, il sera impossible de trouver deux nombres x et y premiers entre eux, tels que :

$$(a) \quad x^5 \pm y^5 = 2^m 5^n A z^{5, k}$$

Supposons, contre l'énoncé du théorème, que l'équation soit possible. Comme le second membre est pair (m ayant été supposé > 0), il faut que les nombres x et y , qui sont premiers entre eux soient impairs l'un et l'autre. Si

nous faisons $x \pm y = 2p$, $x \mp y = 2q$, et par suite :

$$x = p+q, \quad \pm y = p-q,$$

les nombres p et q seront entiers, premiers entre eux, et de plus l'un pair, l'autre impair. En substituant les valeurs précédentes de x et $\pm y$ dans l'équation (α), on la changera en celle-ci :

$$2p(p^4+10p^2q^2+5q^4) = 2^m 5^n A z^5.$$

Le premier membre ne peut être égal au second membre, qui est divisible par 5, qu'autant qu'on suppose p divisible par 5. Faisant donc $p = 5r$, nous aurons :

$$2.5^2 r(q^4+2.5^2 q^2 r^2+5^3 r^4) = 2^m 5^n A z^5.$$

Le nombre n est, par hypothèse, égal à l'unité ou plus grand que 2. Si n est égal à l'unité, il faudra, dans l'équation précédente, supposer z divisible par 5. On pourra, dans ce cas, mettre $5z$ à la place de z , ou, ce qui est la même chose, donner à 5 l'exposant 6, d'où l'on voit que l'on peut supposer, dans tous les cas, $n > 2$. Si l'on met maintenant l'équation précédente sous cette forme :

$$r(q^4+2.5^2 q^2 r^2+5^3 r^4) = 2^{m-1} 5^{n-2} A z^5,$$

et qu'on se rappelle que les nombres q et $p = 5r$ sont premiers entre eux, et de plus l'un pair l'autre impair, il sera facile de voir que le facteur trinôme est impair, non-divisible par 5 et premier à r ; il faut donc que r soit divisible par 5, n étant > 2 . Choisissons actuellement deux nombres positifs, μ et ν , tels que *) $m + \mu - 1$, $n + \nu - 2$, soient divisibles par 5, et un nombre B qui n'ait d'autres diviseurs premiers que ceux du nombre A et tel que le produit AB soit une cinquième puissance. Si nous multiplions l'équation précédente par $2^\mu 5^\nu B$, nous aurons :

$$2^\mu 5^\nu B r(q^4+2.5^2 q^2 r^2+5^3 r^4) = 2^{m+\mu-1} 5^{n+\nu-2} A B z^5.$$

Le second membre de cette équation étant une cinquième puissance, le premier membre en sera pareillement une. Or je dis que les deux facteurs dans lesquels ce premier membre peut se décomposer, le facteur $2^\mu 5^\nu B r$ et le facteur trinôme, sont premiers entre eux. En effet, nous avons déjà vu plus haut que le facteur trinôme est premier à $2^\mu 5^\nu r$, et il résulte d'un autre

*) Si $m-1$ était divisible par 5, on choisirait pour μ une autre valeur que zéro pour éviter les exposants négatifs dans ce qui va suivre.

côté des théorèmes connus d'EULER sur la forme linéaire des diviseurs premiers de la formule $x^n \pm y^n$ (*Théorie des nombres*, no. 156) que le facteur trinôme, dans lequel q et r n'ont pas de diviseur commun, n'est divisible que par des nombres premiers de la forme $10k+1$, qui, d'après les suppositions faites dans l'énoncé du théorème, ne convient à aucun des diviseurs de A , et par conséquent aussi de B , B n'ayant pas d'autres diviseurs premiers que ceux du nombre A . Il faut donc que le nombre $2^{\mu}5^{\nu}Br$ et le facteur trinôme soient des cinquièmes puissances l'un et l'autre.

Le facteur trinôme pouvant s'écrire de cette manière :

$$(q^2 + 5^2 r^2)^2 - 5(10r^2)^2,$$

et les nombres $q^2 + 5^2 r^2$, $10r^2$ étant premiers entre eux, le premier impair, le second pair et divisible par 5, il suffira, en vertu du théorème I., pour égaliser le facteur trinôme avec toute la généralité convenable à une cinquième puissance, de poser ces deux équations :

$$\begin{aligned} q^2 + 5^2 r^2 &= t(t^4 + 2 \cdot 5^2 t^2 s^2 + 5^3 s^4), \\ 10r^2 &= 5s(t^4 + 10t^2 s^2 + 5s^4). \end{aligned}$$

Les nombres s et t doivent être supposés premiers entre eux, et de plus le premier pair, le second impair et non-divisible par 5. Il suit de là que s doit être divisible par 5; en effet t n'étant pas divisible par 5, le second membre de la seconde équation ne peut être divisible par 5^2 qu'autant que s est divisible par 5; mais le premier membre qui a r^2 pour facteur, est divisible par 5^2 ; donc s est divisible par 5.

Nous avons vu plus haut que $2^{\mu}5^{\nu}Br$ devait être une cinquième puissance. Le nombre $2^{2\mu}5^{2\nu}B^2r^2$, carré du nombre précédent, devra donc être une puissance du même degré, et même du dixième degré. Or, en multipliant par $2^{2\mu-1}5^{2\nu-1}B^2$ les deux membres de la dernière équation, on aura celle-ci :

$$2^{2\mu-1}5^{2\nu}B^2r^2 = 2^{2\mu-1}5^{2\nu}B^2s(t^4 + 10t^2s^2 + 5s^4).$$

Si donc nous faisons pour abrégér: $2\mu-1 = g$, $2\nu = h$, $B^2 = C$, tout se réduira à faire voir qu'il est impossible de trouver deux nombres s et t premiers entre eux, et dont le premier soit de plus pair et divisible par 5, tels que le produit :

$$(\beta) \quad 2^g 5^h C s (t^4 + 10t^2 s^2 + 5s^4)$$

soit une cinquième puissance.

En ayant égard à la nature des diviseurs premiers de C , on s'assurera facilement que le facteur $2^g 5^h C s$ et le facteur trinôme sont premiers entre eux. Il faudrait donc, pour que le produit (β) pût être une cinquième puissance, que chacun de ces facteurs en fût pareillement une. Le facteur trinôme peut s'écrire de cette manière:

$$(t^2 + 5s^2)^2 - 5(2s^2).$$

Comme les nombres $t^2 + 5s^2$ et $2s^2$ sont évidemment premiers entre eux, et de plus le premier impair et le second pair et divisible par 5, le théorème I. est applicable ici, et l'on pourra poser:

$$\begin{aligned} t^2 + 5s^2 &= t'(t'^4 + 2 \cdot 5^2 t'^2 s'^2 + 5^3 s'^4), \\ 2s^2 &= 5s'(t'^4 + 10t'^2 s'^2 + 5s'^4). \end{aligned}$$

Les nombres s' et t' doivent être supposés premiers entre eux, et de plus le premier pair, le second impair et non-divisible par 5. Comme t' n'est pas divisible par 5, il est évident par la seconde équation, dont le premier membre renferme le facteur s^2 et est par conséquent divisible par 5^2 , que s' doit être divisible par 5. Ainsi les nombres s' et t' sont premiers entre eux, de même que les nombres s et t , et le premier s' est en outre pair et divisible par 5 comme s .

Il est facile encore de voir que s' est plus petit que s : car on conclut immédiatement de la dernière équation $5^2 s'^5 < 2s^2$ et par suite $s' < \sqrt[5]{\frac{2s^2}{25}}$.

On a vu plus haut que $2^g 5^h C s$ devait être une cinquième puissance. Le nombre $2^{2g} 5^{2h} C^2 s^2$, carré du précédent, devra donc être une puissance du même degré. Or, en multipliant les deux membres de la dernière équation par $2^{2g-1} 5^{2h} C^2$, on aura:

$$2^{2g} 5^{2h} C^2 s^2 = 2^{2g-1} 5^{2h+1} C^2 s' (t'^4 + 10t'^2 s'^2 + 5s'^4),$$

ou, ce qui est la même chose, en faisant $2g-1 = g'$, $2h+1 = h'$, $C^2 = C'$, dans le second membre:

$$(\beta') \quad 2^{2g} 5^{2h} C^2 s^2 = 2^{g'} 5^{h'} C' s' (t'^4 + 10t'^2 s'^2 + 5s'^4),$$

équation dont les deux membres doivent être des puissances du cinquième degré.

Nous voilà donc arrivé à un produit (β') semblable au produit (β) , mais dans lequel le nombre s' est plus petit que le nombre s du produit (β) , et ce produit (β') serait une cinquième puissance, si le produit (β) en était

une. En traitant le produit (β') comme nous avons traité le produit (β) , on arriverait à un troisième produit (β'') , dans lequel le nombre s'' serait plus petit que s' , et l'on pourrait continuer ce procédé aussi loin que l'on voudrait. Il est facile de voir en outre que quelque loin que l'on prolonge les séries $s, s', s'', \dots; t, t', t'', \dots$ on ne pourra jamais rencontrer un terme égal à zéro: car il est évident que si l'on supposait nul un de ces termes, on conclurait en remontant que $s = 0$, cas évident, et qui d'ailleurs est exclu, puisque les nombres s et t ont été supposés premiers entre eux.

Si donc le produit (β) pouvait être une cinquième puissance, on pourrait obtenir, par l'analyse précédente, une suite indéfinie de nombres entiers positifs, dans laquelle chaque terme serait plus petit que le terme précédent, sans qu'aucun des termes fût nul; ce qui implique contradiction. On doit conclure de là que le produit (β) ne saurait être une puissance du cinquième degré.

Le théorème V. se trouvant ainsi établi, nous allons donner le moyen d'en déduire un autre plus général. Considérons l'équation:

$$x^5 \pm y^5 = 2^m A z^5,$$

dans laquelle nous supposons x et y premiers entre eux, $m \geq 0$, et A soumis aux mêmes restrictions que dans l'énoncé du théorème V. Soient α, β, γ des nombres positifs moindres que 5, et tels que $x \equiv \alpha, \pm y \equiv \beta, z \equiv \gamma \pmod{5}$, et soit encore H un nombre positif < 25 et tel que $2^m A \equiv H \pmod{25}$. Comme 5 est un nombre premier, on aura:

$$x^5 \equiv x, \quad y^5 \equiv y, \quad z^5 \equiv z \pmod{5}.$$

On conclut de là, en ayant égard à l'équation posée plus haut:

$$x \pm y \equiv 2^m A z \pmod{5},$$

et partant:

$$\alpha + \beta \equiv H \gamma \pmod{5}.$$

Comme α est le reste de x , on pourra poser $x = \alpha + 5k$, k étant un entier: on tire de là, en élevant les deux membres à la cinquième puissance:

$$x^5 = \alpha^5 + 5\alpha^4(5k) + \frac{5 \cdot 4}{1 \cdot 2} \alpha^3(5k)^2 + \text{etc.},$$

on aura donc:

$$x^5 \equiv \alpha^5 \pmod{25}.$$

On trouvera de la même manière $\pm y^5 \equiv \beta^5$, $z^5 \equiv \gamma^5 \pmod{25}$, et comme on a aussi $2^m A \equiv H \pmod{25}$, on obtiendra, en ayant égard à l'équation citée:

$$\alpha^5 + \beta^5 \equiv H\gamma^5 \pmod{25}.$$

Si maintenant, en substituant dans cette congruence successivement pour α , β toutes les combinaisons que l'on peut former avec les nombres positifs moindres que 5, et pour γ les valeurs correspondantes également moindres que 5, données par la formule:

$$\alpha + \beta \equiv H\gamma \pmod{5},$$

on trouve que la congruence $\alpha^5 + \beta^5 \equiv H\gamma^5 \pmod{25}$ ne peut subsister que lorsque γ est nul, on sera assuré que l'équation:

$$x^5 \pm y^5 = 2^m Az^5$$

ne peut avoir lieu, à moins qu'on ne suppose z divisible par 5. On pourra donc, dans ce cas, mettre $5z$ à la place de z , ce qui change notre équation en celle-ci:

$$x^5 \pm y^5 = 2^m 5^5 Az^5,$$

qui rentre évidemment dans le théorème II., et par conséquent est impossible. Or ce cas a lieu toutes les fois que le nombre H est un des huit nombres suivants 3, 4, 9, 12, 13, 16, 21, 22, comme on peut s'en assurer par un calcul très simple. Nous avons donc ainsi ce nouveau théorème:

Théorème VI.

„Les nombres m et A étant soumis aux mêmes restrictions que dans l'énoncé du théorème II., si le nombre $2^m A$, étant divisé par 25, donne un des huit restes suivants, 3, 4, 9, 12, 13, 16, 21, 22, il sera impossible de trouver deux nombres x et y premiers entre eux, tels que l'on ait $x^5 \pm y^5 = 2^m Az^5$.”

Pour donner un exemple bien simple, considérons les deux équations:

$$x^5 \pm y^5 = 4z^5, \quad x^5 \pm y^5 = 16z^5.$$

Comme dans ces équations on peut, sans nuire à la généralité, supposer les nombres x et y premiers entre eux, il sera facile de voir qu'elles rentrent dans le théorème II. En effet, si l'on fait $A = 1$, et successivement $m = 2$, $m = 4$, on aura respectivement:

$$2^m A = 4, \quad 2^m A = 16.$$

Il est donc prouvé que les deux équations précédentes sont impossibles.

Considérons encore l'équation:

$$x^5 \pm y^5 = z^5,$$

qui est une de celles que FERMAT a assuré être impossibles. Par des considérations semblables à celles qui nous ont servi pour établir le théorème précédent, on peut s'assurer que cette équation ne saurait subsister, à moins qu'une des indéterminées x, y, z ne soit divisible par 5. Soit z l'indéterminée divisible par 5, car il est évident qu'on peut faire en sorte qu'une quelconque des indéterminées se trouve toute seule dans un membre. D'un autre côté, si l'on suppose ces indéterminées premières entre elles, l'une d'elles sera paire et les deux autres seront impaires. Si z était paire, on pourrait remplacer cette indéterminée par $2.5.z$, ce qui changerait l'équation précédente en celle-ci:

$$x^5 \pm y^5 = 2^5 5^5 z^5,$$

qui est impossible, puisqu'elle rentre évidemment dans le théorème II. Il ne resterait donc qu'à traiter le cas où l'indéterminée divisible par 5 serait impaire; mais la méthode exposée dans ce Mémoire paraît insuffisante pour ce cas, et je ne vois pas comment on pourrait compléter la démonstration du cas particulier du théorème de FERMAT, dont il vient d'être question.

ADDITION AU MÉMOIRE PRÉCÉDENT.

Depuis que le Mémoire précédent a été présenté à l'Académie, M. LEGENDRE a publié un second supplément à sa Théorie des Nombres, dans lequel il démontre l'impossibilité de l'équation:

$$x^5 \pm y^5 = z^5.$$

Le cas de l'indéterminée divisible en même temps par 2 et par 5, est traité dans cet ouvrage comme dans le Mémoire précédent, et l'auteur prouve ensuite l'impossibilité de l'autre cas au moyen d'une analyse nouvelle. L'objet de cette addition est d'établir deux théorèmes nouveaux sur les équations indéterminées du cinquième degré et qui comprennent, comme cas particulier, le théorème de FERMAT pour les cinquièmes puissances. J'y parviens en partant des résultats obtenus dans ce qui précède et en faisant usage d'une analyse qui diffère à plusieurs égards de celle de M. LEGENDRE et qui est entièrement analogue à la méthode exposée dans le Mémoire précédent. On a vu que le succès de l'analyse

que nous y avons employée, est fondé sur ce que, pour égaler à une cinquième puissance impaire le binôme $P^2 - 5Q^2$, dans lequel Q doit être divisible par 5, il suffit de poser:

$$P + Q\sqrt{5} = (g + \psi\sqrt{5})^5,$$

parce que cette circonstance donne lieu à la reproduction continue de l'expression que nous avons appelée facteur trinôme. En traitant les nouvelles équations qui font l'objet de cette addition, on est également conduit au binôme $P^2 - 5Q^2$, Q étant toujours divisible par 5; mais il y a cette différence que les nombres P et Q , qui précédemment étaient l'un pair, l'autre impair, sont ici impairs tous les deux et que le binôme $P^2 - 5Q^2$, qui dans l'autre cas devait être une cinquième puissance impaire, doit être égalé ici au quadruple d'une pareille puissance. Or la formule qui satisfait de la manière la plus générale à cette dernière condition, est susceptible d'être rendue parfaitement semblable à celle qui sert à remplir la première; car j'ai remarqué qu'on peut la présenter de cette manière:

$$P + Q\sqrt{5} = \frac{(g + \psi\sqrt{5})^5}{16},$$

expression qui ne se distingue du résultat qu'on vient de rappeler qu'en ce que les indéterminées g et ψ , au lieu d'être l'une paire, l'autre impaire, doivent être impaires toutes les deux. Dès qu'on a fait cette remarque et qu'en traitant les nouvelles équations qui vont nous occuper, on est arrivé au binôme qu'il s'agit d'égaliser au quadruple d'une cinquième puissance, on voit d'un seul coup d'oeil qu'on doit réussir à prouver l'impossibilité de ces équations, en faisant usage d'un procédé tout à fait analogue à la marche que nous avons suivie dans la démonstration du théorème V. — Nous allons maintenant entrer en matière en commençant par établir la proposition que nous avons déjà énoncée.

Les nombres P et Q , dont le premier est supposé n'être pas divisible par 5, étant impairs tous les deux, et n'ayant pas de diviseur commun, le nombre $P^2 - 5Q^2$ sera de la forme $8k + 4$, et l'on pourra faire:

$$P^2 - 5Q^2 = 4L,$$

L étant un nombre impair et non-divisible par 5. Si nous multiplions membre à membre l'équation précédente et celle-ci:

$$3^2 - 5.1^2 = 4.$$

nous aurons:

$$(3P \pm 5Q)^2 - 5(P \pm 3Q)^2 = 16L.$$

Comme les nombres P et Q sont impairs tous les deux, il est évident qu'en déterminant convenablement le signe, les expressions:

$$\frac{3P \pm 5Q}{4}, \quad \frac{P \pm 3Q}{4}$$

seront entières l'une et l'autre: faisant en conséquence:

$$\frac{3P \pm 5Q}{4} = P', \quad \frac{\pm(P \pm 3Q)}{4} = Q',$$

le signe en dehors de la parenthèse étant choisi de manière à donner une valeur positive pour Q' . L'équation obtenue plus haut se changera en celle-ci: $P'^2 - 5Q'^2 = L$, et l'on s'assurera facilement que l'on a:

$$P + Q\sqrt{5} = (P' \pm Q'\sqrt{5})(3 \pm \sqrt{5}),$$

les signes étant convenablement choisis, et que les nombres P' et Q' sont premiers entre eux, et de plus l'un pair, l'autre impair.

Supposons maintenant que le nombre L doive être une cinquième puissance. On satisfera à cette condition de la manière la plus générale en posant:

$$P' + Q'\sqrt{5} = (M \pm N\sqrt{5})^5 (9 \pm 4\sqrt{5})^p.$$

En substituant cette valeur dans la dernière équation, on aura celle-ci:

$$P + Q\sqrt{5} = (M \pm N\sqrt{5})^5 (9 \pm 4\sqrt{5})^p (3 \pm \sqrt{5}),$$

dans laquelle les signes sont indépendants, comme dans les deux équations précédentes. On peut faire $p = 5k \pm r$, k étant entier et positif, et r ayant une des trois valeurs 0, 1, 2, la quantité $(9 \pm 4\sqrt{5})^p$ se décomposera ainsi en deux facteurs $(9 \pm 4\sqrt{5})^{5k}$ et $(9 \pm 4\sqrt{5})^{\pm r}$ dont le premier peut être omis parce qu'il rentre dans $(M \pm N\sqrt{5})^5$. Si nous observons de plus qu'en vertu de l'équation:

$$9 \pm 4\sqrt{5} = (9 \mp 4\sqrt{5})^{-1}$$

on peut changer dans $(9 \pm 4\sqrt{5})^{\pm r}$ simultanément les signes de r et du radical, nous pouvons supposer r positif, et l'équation donnée plus haut deviendra:

$$P + Q\sqrt{5} = (M \pm N\sqrt{5})^5 (9 \pm 4\sqrt{5})^r (3 \pm \sqrt{5}).$$

L devant toujours être la cinquième puissance d'un nombre impair et non-

divisible par 5, déterminons les conditions nécessaires pour que Q soit divisible par 5. Comme le coefficient de $\sqrt{5}$ dans le développement de $(M \pm N\sqrt{5})^5$ est divisible par 5, et que la partie rationnelle de ce développement ne l'est pas. M n'étant pas divisible par 5, on conclut, comme dans la démonstration du théorème IV., qu'il faut, pour que Q puisse être divisible par 5, que le coefficient de $\sqrt{5}$, dans la valeur développée de $(9 \pm 4\sqrt{5})(3 \pm \sqrt{5})$ le soit.

Or, en substituant pour r successivement les trois valeurs 0, 1, 2, on trouve que cela n'a lieu que dans le cas de $r = 2$, les signes des radicaux dans les deux facteurs $(9 \pm 4\sqrt{5})^r$ et $(3 \pm \sqrt{5})$ étant en même temps opposés. Si l'on fait attention que l'on a :

$$\frac{(3 \pm \sqrt{5})^3}{2^3} = 9 \pm 4\sqrt{5} \quad \text{et} \quad 3 \mp \sqrt{5} = \frac{4}{3 \pm \sqrt{5}},$$

on trouvera que le produit précédent sera, dans le cas dont il s'agit, équivalent à :

$$\frac{(3 \pm \sqrt{5})^5}{2^4},$$

valeur dont la substitution dans l'équation obtenue plus haut, la change en celle-ci :

$$P + Q\sqrt{5} = \frac{(M \pm N\sqrt{5})^5 (3 \pm \sqrt{5})^5}{2^4}.$$

Les nombres M et N étant l'un pair, l'autre impair, les nombres φ et ψ déterminés par l'équation :

$$\varphi + \psi\sqrt{5} = (M \pm N\sqrt{5})(3 \pm \sqrt{5})$$

seront impairs l'un et l'autre, et l'on aura :

$$P + Q\sqrt{5} = \frac{(\varphi + \psi\sqrt{5})^5}{2^4}$$

et par conséquent :

$$P = \varphi \frac{(\varphi^4 + 2 \cdot 5^2 \varphi^2 \psi^2 + 5^3 \psi^4)}{2^4},$$

$$Q = 5\psi \frac{(\varphi^4 + 10\varphi^2 \psi^2 + 5\psi^4)}{2^4}.$$

Pour que P et Q soient premiers entre eux, il faut que φ et ψ n'aient pas de

diviseur commun, et que le premier de ces nombres ne soit pas divisible par 5, et réciproquement, si les nombres g et ψ , dont le premier est supposé ne pas être divisible par 5, n'ont pas de diviseur commun et sont impairs l'un et l'autre, les nombres P et Q seront entiers et premiers entre eux. En effet, le quart de la quantité $g^4 + 10g^2\psi^2 + 5\psi^4$ pouvant se mettre sous la forme:

$$\left(\frac{g^2 + 5\psi^2}{2}\right)^2 - 5(\psi^2)^2,$$

et cette dernière expression étant évidemment le quadruple d'un nombre impair, on voit que la valeur de Q est entière et impaire; la même chose se prouvera pour la valeur de P , et l'on s'assurera facilement que les nombres P et Q , qui sont impairs tous les deux, n'ont pas de diviseur commun. Nous avons donc ainsi ce théorème:

Théorème VII.

Les nombres P et Q devant être premiers entre eux, impairs l'un et l'autre, et le dernier devant être divisible par 5, je dis que pour égaler le binôme $P^2 - 5Q^2$ au quadruple d'une cinquième puissance avec toute la généralité convenable, il suffira de poser:

$$P + Q\sqrt{5} = \frac{(g + \psi\sqrt{5})^5}{2^4},$$

les nombres indéterminés g et ψ étant premiers entre eux, impairs l'un et l'autre et le premier de plus non-divisible par 5*).

Voici maintenant le premier des théorèmes nouveaux que nous avons annoncés au commencement de cette addition.

Théorème VIII.

La lettre n désignant un nombre positif autre que 0 et 2, et le nombre A n'étant divisible ni par 2, ni par 5, ni par aucun nombre premier de la forme $10k + 1$, il sera impossible de trouver deux nombres x et y premiers entre eux et tels que:

$$(y) \quad x^5 \pm y^5 = 5^n A z^{5^n}.$$

Les nombres x et y peuvent être impairs tous les deux, ou l'un pair

*. Ce théorème, comme le théorème IV, a ses analogues pour beaucoup d'autres nombres premiers.

et l'autre impair. Dans le premier cas, z sera divisible par 2, et l'on pourra mettre $2z$ à la place de z , ce qui changera l'équation (γ) en celle-ci :

$$x^5 \pm y^5 = 2^5 5^n A z^5,$$

qui est impossible puisqu'elle rentre évidemment dans le théorème V. Reste donc à prouver l'impossibilité du second cas où l'on suppose les nombres x , y l'un pair, l'autre impair. Si nous faisons :

$$x \pm y = p, \quad x \mp y = q,$$

nous aurons :

$$2x = p + q, \quad \pm 2y = p - q,$$

et les nombres p et q seront premiers entre eux et de plus impairs l'un et l'autre. En substituant les valeurs précédentes de $2x$ et $\pm 2y$ dans l'équation (γ), après en avoir multiplié les deux membres par 2^5 , on aura :

$$p(p^4 + 10p^2q^2 + 5q^4) = 2^4 5^n A z^5.$$

Comme p doit évidemment être divisible par 5, nous ferons $p = 5r$, ce qui donnera :

$$5^2 r(q^4 + 2 \cdot 5^2 q^2 r^2 + 5^3 r^4) = 2^4 5^n A z^5.$$

Le nombre n est par hypothèse égal à l'unité ou plus grand que 2. Si n est égal à l'unité, il faudra, dans l'équation précédente, supposer z divisible par 5. On pourra donc, dans ce cas, mettre $5z$ à la place de z ou, ce qui est la même chose, donner à 5 l'exposant 6, d'où l'on voit que l'on peut supposer dans tous les cas $n > 2$.

Si l'on met l'équation précédente sous cette forme :

$$r(q^4 + 2 \cdot 5^2 q^2 r^2 + 5^3 r^4) = 2^4 5^{n-2} A z^5,$$

et qu'on fasse attention que $n > 2$ et que q est premier à $p = 5r$, on voit que r doit être supposé divisible par 5.

Choisissons maintenant un nombre positif ν tel que $n + \nu - 2$ soit divisible par 5 et un nombre B qui n'ait d'autres diviseurs premiers que ceux du nombre A et tel que le produit AB soit une cinquième puissance. Multipliant la dernière équation par $5^\nu B$, nous aurons :

$$5^\nu B r(q^4 + 2 \cdot 5^2 q^2 r^2 + 5^3 r^4) = 2^4 5^{n+\nu-2} A B z^5.$$

Tous les diviseurs du facteur trinôme, dans lequel q et r sont premiers

entre eux, étant de la forme $10k+1$, il est évident qu'il n'a aucun diviseur commun avec B ; il n'est pas moins évident qu'il est aussi premier à $5^{\nu}r$, et par conséquent à $5^{\nu}Br$.

Comme le facteur $5^{\nu}Br$ et le facteur trinôme sont premiers entre eux et que le premier de ces facteurs est impair, il faut, en vertu de la dernière équation, dont le second membre est le produit de 2^4 et de la cinquième puissance d'un nombre impair, que $5^{\nu}Br$ soit une cinquième puissance, et le facteur trinôme une cinquième puissance multipliée par 2^4 .

Le quart du facteur trinôme devant être le quadruple d'une cinquième puissance, et ce quart pouvant se mettre sous la forme:

$$\left(\frac{q^2+5^2r^2}{2}\right)^2 - 5(5r^2)^2,$$

où les nombres $\frac{q^2+5^2r^2}{2}$, $5r^2$ sont évidemment premiers entre eux, impairs l'un et l'autre et le dernier de plus divisible par 5, il suffira, en vertu du théorème établi au commencement de cette addition, pour égaliser le quart du facteur trinôme au quadruple d'une cinquième puissance, de poser ces deux équations:

$$\frac{q^2+5^2r^2}{2} = t \frac{(t^4+2.5^2t^2s^2+5^3s^4)}{2^4},$$

$$5r^2 = 5s \frac{(t^4+10t^2s^2+5s^4)}{2^4},$$

les nombres indéterminés t et s devant être supposés premiers entre eux, impairs l'un et l'autre et le premier de plus non-divisible par 5. Comme t n'est pas divisible par 5 et que r l'est ainsi que nous l'avons vu ci-dessus, il faut, en vertu de la dernière des équations précédentes, que s soit divisible par 5.

Nous avons vu plus haut que $5^{\nu}Br$ devait être une cinquième puissance. Le nombre $5^{2\nu}B^2r^2$, carré du précédent, devra donc être une puissance du même degré, et même du dixième degré.

Or, en multipliant par $2^4 5^{2\nu-1}B^2$ les deux membres de la dernière équation, on aura celle-ci:

$$2^4 5^{2\nu} B^2 r^2 = 5^{2\nu} B^2 s (t^4 + 10t^2s^2 + 5s^4).$$

Si donc nous faisons pour abrégér $2\nu = h$, $B^2 = C$, tout se réduit à

faire voir qu'il est impossible de trouver deux nombres t et s premiers entre eux, impairs l'un et l'autre, et dont le dernier s soit de plus divisible par 5, tels que le produit:

$$(\delta) \quad 5^h C s (t^4 + 10t^2 s^2 + 5s^4)$$

soit une cinquième puissance multipliée par 2^4 .

Il est facile de voir que l'expression (δ) ne saurait être le produit de 2^4 et d'une cinquième puissance, à moins que $5^h C s$ ne soit une cinquième puissance, et le facteur trinôme une cinquième puissance multipliée par 2^4 .

Le quart du facteur trinôme devant être le quadruple d'une cinquième puissance, et ce quart pouvant se mettre sous la forme:

$$\left(\frac{t^2 + 5s^2}{2} \right)^2 - 5(s^2)^2,$$

où les nombres $\frac{t^2 + 5s^2}{2}$, s^2 sont évidemment premiers entre eux, impairs l'un et l'autre, et le dernier de plus divisible par 5, il suffira, pour égaliser le facteur trinôme divisé par 4 au quadruple d'une cinquième puissance, de poser ces équations:

$$\begin{aligned} \frac{t^2 + 5s^2}{2} &= t' \frac{(t'^4 + 2 \cdot 5^2 t'^2 s'^2 + 5^3 s'^4)}{2^4}, \\ s^2 &= 5s' \frac{(t'^4 + 10t'^2 s'^2 + 5s'^4)}{2^4}, \end{aligned}$$

les nombres t' et s' étant supposés premiers entre eux, impairs l'un et l'autre, et le premier t' de plus non-divisible par 5. Comme s est divisible par 5, et que t' ne l'est plus, il faut, d'après la dernière équation, que s' soit aussi divisible par 5. On conclut encore de la dernière équation qu'on a: $\frac{2 \cdot 5}{16} s'^2 < s^2$ et par suite que s' est beaucoup plus petit que s .

Le nombre $5^h C s$ devant être une cinquième puissance, $5^{2h} C^2 s^2$, carré du nombre précédent, devra être une puissance du même degré et même du dixième degré. Or, en multipliant par $2^4 5^{2h} C^2$ les deux membres de la dernière équation, on aura celle-ci:

$$2^4 5^{2h} C^2 s^2 = 5^{2h+1} C'^2 s' (t'^4 + 10t'^2 s'^2 + 5s'^4)$$

ou, ce qui est la même chose, en faisant $2h+1 = h'$, $C^2 = C'$ dans le second

nombre:

$$(d') \quad 2^3 5^{2h} C^2 s^2 = 5^{h'} C' s' (t'^4 + 10 t'^2 s'^2 + 5 s'^4),$$

équation dont les deux membres devront être des cinquièmes puissances multipliées par 2^3 .

Le produit (d') étant parfaitement semblable au produit (d) , et le nombre s' étant beaucoup plus petit que le nombre s , on conclura, comme dans la démonstration du théorème V. du mémoire précédent, que le produit (d) ne saurait être égal à une cinquième puissance, multipliée par 2^3 , et que par conséquent l'équation (γ) ne saurait avoir lieu.

Le théorème de FERMAT, pour le cas des cinquièmes puissances, est compris comme cas particulier dans le théorème que nous venons d'établir. En effet, l'équation $x^5 \pm y^5 = z^5$ ne pouvant avoir lieu, à moins qu'une des indéterminées, z par exemple, ne soit divisible par 5, nous pouvons mettre $5z$ à la place de z ; ce qui donnera $x^5 \pm y^5 = 5^5 z^5$, équation impossible, puisqu'elle rentre dans le dernier théorème.

Un raisonnement tout-à-fait semblable à celui au moyen duquel nous avons établi le théorème VI., en partant du théorème V., peut servir à déduire du théorème que nous venons de démontrer un nouveau théorème qui peut s'énoncer comme il suit:

Théorème IX.

„Le nombre A étant soumis aux mêmes restrictions que dans l'énoncé du théorème VIII., et ce nombre donnant un des huit restes suivants, 3, 4, 9, 12, 13, 16, 21, 22, lorsqu'il est divisé par 25, il sera impossible de trouver deux nombres x et y premiers entre eux, et tels que l'on ait $x^5 \pm y^5 = Az^5$.”

DE
FORMIS LINEARIBUS,

IN QUIBUS CONTINENTUR DIVISORES PRIMI QUARUMDAM
FORMULARUM GRADUUM SUPERIORUM

COMMENTATIO,

QUAM

AD VENIAM DOCENDI

AB AMPLISSIMO PHILOSOPHORUM ORDINE IN REGIA UNIVERSITATE
LITTERARUM VRATISLAVIENSI IMPETRANDAM

CONSCRIPSIT

GUSTAVUS LEJEUNE DIRICHLET,
PHILOSOPHIAE DOCTOR.

Vratislaviae, Typis Kupferianis.

DE FORMIS LINEARIBUS, IN QUIBUS CONTINENTUR DIVISORES PRIMI QUARUNDAM FORMULARUM GRADUUM SUPERIORUM.

Constat e doctrina de residuis quadraticis seu theoria divisorum formularum secundi gradus, divisores primos talium formularum in certis formis linearibus contineri, et esse formas lineares ab illis diversas, in quibus non-divisores sint comprehensi, ita ut ad absolvendam quaestionem, utrum primus datus formulam datam metiatur necne, sufficiat examinare, num primus in aliqua priorum an posteriorum formarum contineatur. Longe aliter res sese habet in formulis gradus superioris, quarum divisores a non-divisoribus simili modo discerni non possunt, et quibus adhibenda sunt criteria ab illis, quae in doctrina de residuis quadraticis proponuntur, longe diversa. Ratio divisores formularum gradus superioris a non-divisoribus distinguendi ut exemplo illustretur, contemplerur formulam quarti gradus $x^4 - 3$. Ex simplicissimis arithmeticae superioris principiis deducitur, hae formulae propositae, solos primos formae $12n + 1$ criterium altioris generis requirere, de reliquis autem ope notae doctrinae de residuis quadraticis rem diiudicari posse. Talis formae si proponitur primus, et quaeritur, utrum formulae $x^4 - 3$ sit divisor necne, hoc criterio erit utendum. Redigatur primus sub formam $t^2 + 3u^2$, quod semper et unico quidem modo fieri posse constat. Tum numerus t , quem nec per 2 nec per 3 divisibilem fore est perspicuum, erit formae $12n \pm 1$, vel formae $12n \pm 5$. Si prior casus locum habet, primus erit divisor formulae $x^4 - 3$, sin posterior, non erit. Est aliud criterium ad eandem quaestionem decidendam idoneum, quod tamen, ut elegantiorum habeat formam, non referendum est ad formulam $x^4 - 3$, sed ad hanc $x^4 + 3$, quae posterior priori tam arcte est coniuncta, ut, si numerum aliquem posterioris divisorem esse vel non esse scimus, inde statim concludi possit, utrum idem numerus priorem metiatur necne. Quod alterum criterium si adhibere velis, numerus primus propositus in duo quadrata est resolvendus. Quadratorum, quae haec decompositio suppeditat, alterum manifesto erit par, alterum

impar, nec minus facile est perspectu, alterum horum quadratorum idque unum tantum per 3 fore divisibile. Quibus ita praeparatis, criterium hoc modo exhiberi licet:

„Si quadratum par per 3 est divisibile, primus metietur formulam x^3+3 , sin impar, non metietur.“

Demonstrationes theorematum modo propositorum invenies in commentationibus nonnullis, in quibus theoriam generalem divisorum formulae $\alpha x^3 + \beta x^2 + \gamma$ struere conabor et quarum prima nuper lucem vidit in cel. CRELLI ephemeridibus mathematicis (Recherches sur les diviseurs premiers d'une classe de formules du quatrième degré. Premier Mémoire). Theoremata praecedentia hoc loco non nisi in hunc finem sunt prolata, ut exemplo aliquo appareat, quantum formulae gradus superioris a formulis quadraticis differre inveniantur, si in divisorum primorum indolem inquiritur. Quae diversitas quamquam in genere valere videtur, sunt tamen formulae particulares cuiusvis fere gradus, quae respectu divisorum simili se habent modo, quo formulae secundi gradus, eoque ut ex forma lineari, in qua continetur primus, cognosci possit, num formulam huius generis metiatur. Ad hoc genus referendae sunt formulae in expressione $x^n \pm 1$ comprehensae, de quibus ill. EULER instituit disquisitiones non minus insignes, quod ratiocinandi methodus, qua vir summus est usus, eximia simplicitate gaudet, quam quod theoremata, quae eius ope stabiliuntur, latissime patent. Quibus ill. EULERI disquisitionibus incumbens, meidi in novam quandam formularum speciem, quae, quod ad divisores attinet, similes habent proprietates, ut in sequentibus sum expositurus.

Cum pars disquisitionum sequentium nonnullis theorematum Eulerianorum modo laudatorum sit superstruenda, utile duximus, theoremata, quibus nobis opus erit, hoc loco in conspectum producere. Demonstrationes brevitatis causa omittimus, lectorem ad ill. EULERI dissertationes vel ill. LEGENDRE opus egregium ablegantem, qui et haec et reliqua EULERI inventa arithmetica summa cum perspicuitate exposuit.

Theorema I. Si p est primus impar, omnes divisores primi formulae $\frac{x^p-1}{x-1}$ in forma lineari $2mp+1$ continentur, et vice versa quivis primus in hac forma comprehensus formulae est divisor.

Theorema II. Si a est potestas numeri 2, divisores formulae x^a+1 continentur in forma $2ma+1$, et vice versa quivis primus huius formae formulam metitur.

Formulae, de quarum divisoribus in sequentibus disquisitionem instituemus, originem trahunt ex evolutione potestatis $(x + \sqrt{b})^n$, ubi n et b sunt integri dati (posterior non-quadratus). x autem designat integrum indeterminatum. Ponamus, evolutione perfecta, prodire $U + V\sqrt{b}$, ubi tam U quam V a quantitate irrationali \sqrt{b} liberi supponuntur, ita ut habeamus:

$$(1) \quad \begin{aligned} (x + \sqrt{b})^n &= U + V\sqrt{b}, & (x - \sqrt{b})^n &= U - V\sqrt{b}, \\ \Gamma &= nx^{n-1} + \frac{n(n-1)(n-2)}{1.2.3}x^{n-3}b + \frac{n(n-1)(n-2)(n-3)(n-4)}{1.2.3.4.5}x^{n-5}b^2 + \dots \end{aligned}$$

Propositum est nobis, definire numeros primos, per quos V fit divisibilis, si ipsi x omnes valores integri tam positivi quam negativi successive tribuuntur. Excipiuntur tantum valores ad ipsum b non primi, quippe qui theorematum concinnitatem turbent. Caeterum facillime perspicitur, casum, ubi x cum ipso b divisorem communem habere statuitur, ad casum, ubi x et b inter se sunt primi, reduci posse.

Ut initium huius disquisitionis faciamus, demonstremus, ipsos U et V nullum divisorem communem (numero 2 excepto) habere posse, quotiescumque x valorem ad ipsum b primum nanciscitur. Ad hanc rem probandam, a suppositione contrarii proficiscimur. Sit igitur δ primus utrumque ipsorum U et V metiens. Si prima aequationum (1) in secundam multiplicatur, prodibit haec:

$$(x^2 - b)^n = U^2 - bV^2,$$

ex cuius inspectione concluditur, primum δ ipsius $x^2 - b$ esse divisorem, quod, si signo ab ill. GAUSS introducto utimur, hoc modo designabimus:

$$x^2 \equiv b \pmod{\delta}.$$

ex qua congruentia hae novae deducuntur:

$$x^4 \equiv b^2, \quad x^6 \equiv b^3, \quad x^8 \equiv b^4, \quad \dots \pmod{\delta}.$$

Si iam in expressione (1) ipsius V loco ipsorum b , b^2 , b^3 , ... valores secundum modulum δ illis resp. congruos x^2 , x^4 , x^6 , ... substituerimus, obtinebimus congruentiam:

$$V \equiv x^{n-1} \left(n + \frac{n(n-1)(n-2)}{1.2.3} + \frac{n(n-1)(n-2)(n-3)(n-4)}{1.2.3.4.5} + \dots \right) \pmod{\delta},$$

quam, cum expressionem unciam inclusam esse $\frac{1}{2}((1+1)^n - (1-1)^n)$ sive 2^{n-1} facillime perspicitur, hoc quoque modo exhibere possumus:

$$V \equiv 2^{n-1}x^{n-1} \pmod{\delta}.$$

Sequitur ex hac congruentia, primum impari δ , quem ipsius V divisorem esse supposuimus, etiam esse divisorem ipsius x . Supra autem vidimus, numerum

$x^2 - b$ per δ esse divisibilem, δ metietur igitur utrumque ipsorum x et b , quod est contra suppositionem, numeros x et b inter se esse primos. Concludendum est igitur, suppositionem, ipsos U et V habere divisorem communem imparem, constare non posse.

His praemissis, in indolem divisorum primorum formulae V inquiremus. Quamquam methodus, qua in hac disquisitione utemur, pro quovis valore ipsius n applicari potest, hoc loco, ne haec dissertatio nimis longa fiat, duos tantum casus examini subiciemus, quorum prior locum habet, quando n est primus impar, posterior, quando n est potestas numeri 2.

Sit igitur primo n numerus primus impar, quem per litteram p designabimus, et k primus impar ab ipso p diversus formulam V metiens. Iam duo casus sunt distinguendi, prout b ipsius k est residuum aut non-residuum quadraticum.

Casu priore datur numerus μ hinc congruentiae $\mu^2 \equiv b \pmod{k}$ satisfaciens. Primus k , quem formulae V divisorem esse statuimus, eandem metietur, si loco ipsius b valorem secundum modulum k congruum μ^2 substituerimus.

Formula V , quae primam et secundam aequationem (1) comparando hoc modo exhiberi posse invenitur:

$$\frac{(x+\sqrt{b})^p - (x-\sqrt{b})^p}{2\sqrt{b}},$$

substitutione, quam diximus, perfecta, in hanc abit:

$$\frac{(x+\mu)^p - (x-\mu)^p}{2\mu},$$

in qua expressione neutrum numerorum $x+\mu$ et $x-\mu$ per k divisibilem esse dico. Si enim alter esset, alter non esset, $(x+\mu)^p - (x-\mu)^p$ per k non foret divisibilis. Utrumque autem per k divisibilem esse non posse hoc modo demonstratur. Tum enim k metiretur etiam utrumque ipsorum:

$$\frac{1}{2}((x+\mu)+(x-\mu)) \quad \text{et} \quad \frac{1}{2}((x+\mu)-(x-\mu)).$$

id est utrumque numerorum x et μ , et quoniam $\mu^2 \equiv b \pmod{k}$ est, k foret quoque divisor ipsius b . Numeri x et b haberent igitur divisorem communem k contra ea quae supposuimus.

Cum neuter ipsorum $x+\mu$ et $x-\mu$ per k sit divisibilis, congruentiae:

$$(x-\mu)y \equiv x+\mu \pmod{k}$$

satisfieri poterit per numerum y .

Quodsi iam in valore ipsius $2\mu V$ loco ipsius $x+\mu$ numerum congruum $y(x-\mu)$ substituerimus, habebimus hanc expressionem per k divisibilem:

$$(x-\mu)^p(y^p-1),$$

et cum $x-\mu$, ut supra vidimus, per k non sit divisibilis, y^p-1 ipsius k multipulum esse concluditur. Iam dico, numerum $y-1$ per k divisibilem non esse; si enim k ipsum $y-1$ metiretur, haberemus $y \equiv 1 \pmod{k}$ et congruentia $(x-\mu)y \equiv x+\mu \pmod{k}$ in hanc transiret $2\mu \equiv 0 \pmod{k}$, id est, μ seu b per k foret divisibilis. Sequitur autem ex inspectione formulae V , k ipsius b divisorem esse non posse, nisi vel k ipsi p sit aequalis, vel ipsum x metiatur; quorum casuum utrumque supra exclusimus. Concluditur iam ope theorematis I, primum k esse formae $2mp+1$.

Habemus igitur theorema: „Nullus primus, cuius residuum est b , formulam V metiri potest, nisi in forma $2mp+1$ contineatur.“ Haec propositio etiam inversa valet et demonstrari potest, quemvis primum formae $2mp+1$ formulae V esse divisorem. Cuius propositionis demonstrationem, cum nulli difficultati sit obnoxia, brevitatis causa omittimus.

Pergimus iam ad primos, quorum non-residuum est b , quorumque relatio ad formulam V (quatenus formulae sunt divisores aut non-divisores) per theoremata sequentia definitur:

„Si primus, cuius non-residuum est b , simul est formae $2mp-1$, formulae V erit divisor.“

„Nullus primus k , cuius non-residuum est b , formulam V metiri potest, nisi in forma $2mp-1$ contineatur.“

Prius horum theorematum iam olim ab ill. LAGRANGE propositum et demonstratum est in commentatione in collectione academica (Nouveaux Mémoires de Berlin, année 1775) conservata, ubi eius ope propositiones nonnullae particulares ad doctrinam de residuis quadraticis pertinentes stabiliuntur. Theorema et demonstratio, qua a viro summo munitum est, exstant etiam in opere egregio „Disquisitiones arithmeticae“, quod cum in manibus omnium versetur, qui analysi Diophantaeae operam navant, demonstrationem hoc loco adicere opus non esse duximus. —

Theorema posterius, quod est prius inversum, a nemine hucusque, quantum scio, est prolatum. Demonstratio minus obvia absolvitur per ratiocinia iis simillima, quibus iam alio loco (Mémoire sur l'impossibilité de quelques équations du cinquième degré) in argumento longe diverso usus sum.

Contemplerur formulam $(x+\sqrt{b})^{k+1}$ et ponamus ex eius evolutione oriri $M+N\sqrt{b}$, ubi M et N a quantitate irrationali \sqrt{b} sunt liberi. Valorem ipsius

N , qui obtinetur, si $k+1$ loco ipsius n in expressione (1) ipsius V substituitur, brevitatis causa non apponimus. Perspicuum est, coefficientes omnium terminorum ipsius N per k esse divisibiles, coefficientibus primi et ultimi termini exceptis.

Qui termini quum sint $(k+1)x^k$ et $(k+1)xb^{\frac{k-1}{2}}$, invenitur:

$$N \equiv (k+1)(x^k + xb^{\frac{k-1}{2}}) \pmod{k}.$$

Constat, numerum b , quem ipsius k non-residuum esse supposuimus, satisfacturum esse congruentiae $b^{\frac{k-1}{2}} \equiv -1 \pmod{k}$, et cum habeamus quoque $x^k \equiv x \pmod{k}$, concluditur:

$$x^k + xb^{\frac{k-1}{2}} \equiv 0 \pmod{k}.$$

N igitur per k erit divisibilis, quicumque valor ipsi x tribuatur.

Ponamus iam, formulam V pro valore determinato ipsius x divisibilem fieri per primum k , cuius non-residuum est b , talemque primum esse formae $2mp-1$ demonstrare conemur.

Cum V per k sit divisibilis, formula U non erit divisibilis, quippe quam formulam ad V primam esse vidimus, dummodo ipsi x valor ad valorem ipsius b primus tribuatur, quod semper fieri supposuimus. Demonstrandum iam est, primum k esse formae $2mp-1$ seu $k+1$ per p esse divisibilem.

Numerus $k+1$ si per p non esset divisibilis, darentur numeri integri g et h positivi ita comparati, ut esset $g(k+1) - hp = 1$.

Revertamur nunc ad contemplationem formulae $M + N\sqrt{b}$, in qua N per k divisibilem esse vidimus, eamque ad potestatem g^{mi} gradus elevemus. Quae potestas si per $M' + N'\sqrt{b}$ designatur, facillime perspicitur N' per N ideoque per k esse divisibilem: M' autem per k non divisibilem esse sequitur ex eo, quod $M' + N'\sqrt{b}$ est potestas ipsius $x + \sqrt{b}$ (cuius potestatis exponents est $g(k+1)$), quam ob rem M' et N' divisorem communem habere non possunt. Eodem modo probatur, si ponatur $(U + V\sqrt{b})^h = U' + V'\sqrt{b}$, V' per k divisibilem fore, U' autem non fore. Ex comparatione aequationum:

$$(x + \sqrt{b})^{g(k+1)} = M' + N'\sqrt{b}, \quad (x + \sqrt{b})^{hp} = U' + V'\sqrt{b}, \quad g(k+1) - hp = 1$$

deducitur haec:

$$(x + \sqrt{b})(U' + V'\sqrt{b}) = M' + N'\sqrt{b},$$

quae, multiplicatione perfecta et partibus rationalibus et coefficientibus ipsius \sqrt{b} separatim aequatis, has novas suppeditat:

$$M' = U'x + bV', \quad N' = U' + V'.$$

Manifestum est, posteriorem harum aequationum locum habere non posse, cum N' et V' ipsius k sint multipla, U' autem per k non sit divisibilis. Concludendum igitur est, suppositionem, a qua profecti sumus, constare non posse, et $k+1$ re vera per p esse divisibilem, seu quod est idem, k esse formae $2mp-1$, q. e. d.

Si ea, quae hucusque docuimus, cum doctrina nota de residuis quadraticis iunguntur, assignari poterunt formae lineares, in quibus divisores primi formulae V includuntur.

Quod ut exemplis illustretur, sit $p = 5$ et $b = -1$: quo casu V invenitur esse $5x^4 - 10x^2 + 1$.

Sequitur ex iis, quae supra demonstravimus, primos, quorum residuum est -1 , ipsius V divisores esse non posse, nisi sint formae $10m+1$, constatque e doctrina de residuis quadraticis primos, quorum residuum est -1 , in forma $4n+1$ contineri. Numeri autem simul in utraque formarum $10m+1$, $4n+1$ inclusi sunt formae $20h+1$, in qua igitur continetur quisque primus, cuius residuum est -1 , et qui simul formulam V metitur.

Ad divisores primos ipsius V , quorum non-residuum est -1 , quod attinget, simili modo invenitur, omnes tales primos in forma $20h-1$ comprehensos esse.

Formula duplex $20h \pm 1$ suppeditat igitur omnes primos expressionem $5x^4 - 10x^2 + 1$ metientes et vice versa quivis primus in altera formarum $20h+1$, $20h-1$ inclusus ipsius V erit divisor.

Exemplum secundum praebebunt suppositiones $p = 7$, $b = 2$: quo casu erit:

$$V = 7x^6 + 70x^4 + 84x^2 + 8.$$

Primi, quorum residuum est 2 , continentur in formis $8m+1$, $8m+7$; huiusmodi autem primi formulam V metiri non possunt, nisi sint formae $14n+1$, quam cum praecedentibus comparando inveniuntur formae $56h+1$, $56h+15$, in quibus includuntur primi, qui ipsius V sunt divisores et quorum simul residuum est 2 .

Primi expressionis V divisores, quorum non-residuum est 2 , in formis $56h+13$, $56h+27$ comprehensi esse inveniuntur.

Formulae $56h+1$, 13 , 15 , 27 suppeditant igitur omnes primos, quadrimonium $7x^6 + 70x^4 + 84x^2 + 8$ metientes, et vice versa quivis primus in una harum formarum contentus quadrimonii erit divisor.

Sunt casus particulares ob theorematum elegantiam attentionem peculiarem merentes. Hos casus, qui locum habent, quoties b ipsi p positive vel negative sumpto aequatur, iam fusius tractabimus.

Sit primo $b = p$: et primum p formae $4n+1$ esse supponatur. Notum est, primos, quorum residuum est $b = p$, in $\frac{1}{2}(p-1)$ huiusmodi formis linearibus contineri:

$$(2) \quad mp+1, \quad mp+a, \quad mp+a', \quad mp+a'', \quad \dots$$

ubi numeri $1, a, a', a'', \dots$, quos positivos ipsoque p minores supponere licet, omnes inter se erunt diversi et e divisione quadratorum $1, 2^2, 3^2, \dots (\frac{1}{2}(p-1))^2$ per primum p oriuntur, inter quos numeros constat numerum $p-1$ occurrere, quoties p est formae $4n+1$. Primi autem, quorum non-residuum est b , continentur in $\frac{1}{2}(p-1)$ aliis formis linearibus:

$$(3) \quad mp+\beta, \quad mp+\beta', \quad mp+\beta'', \quad \dots$$

ubi numeri $\beta, \beta', \beta'', \dots$ qui ipso p minores supponuntur, tam inter se quam ab illis $1, a, a', a'', \dots$ erunt diversi, ita ut numerus $p-1$ inter ipsos $\beta, \beta', \beta'', \dots$ occurrere non possit.

Supra demonstravimus, primum, cuius residuum est b , et qui igitur in aliqua formarum (2) continetur, ipsius V divisorem esse non posse, nisi sit formae $mp+1$, quae est eadem ac prima formarum (2) et cum nulla reliquarum constare potest. Sequitur inde, primos, quorum residuum est $b = p$, et qui simul formulam V metiuntur, in forma $mp+1$ comprehensos esse, et vice versa etc.

Quod ad primos attinet, quorum non-residuum est $b = p$, et qui igitur in aliqua formarum (3) continentur, sequitur ex iis, quae supra stabilivimus, tales primos formulae V divisores esse non posse, nisi simul in forma $mp-1$ seu, quod est idem, in forma $mp+p-1$ includantur. Haec autem forma cum nulla formarum (3) constare potest, quia nullus numerorum $\beta, \beta', \beta'', \dots$ ipsi $p-1$ est aequalis.

Probatum igitur est, nullum primum, cuius non-residuum sit $b = p$, ipsius V esse divisorem, omnesque primos formulam V metientes in forma $mp+1$ esse comprehensos.

Si casus, ubi $b = -p$, p designante primum formae $4m+1$, simili modo examinatur, invenitur, nullum primum, nisi in altera formarum $4mp \pm 1$ contineatur, formulae V divisorem esse posse, et vice versa quemvis primum in altera harum formarum inclusum re vera formulam V metiri.

Casus tertius locum habet, quando $b = p$, et p est formae $4m+3$. Hoc

casu primi formulam V metientes in formis $4mp+1$, $4mp+2p-1$ comprehensi esse inveniuntur.

Superest, ut casum quartum examini subiciamus. Primus p hoc casu est formae $4m+3$, et b ipsi p negative sumpto est aequalis. Si considerationes, quibus in casibus praecedentibus usi sumus, ad casum praesentem applicaverimus, perveniemus ad hoc theorema:

Nullus primus formulam V , in qua $b = -p$ et p primum formae $4m+3$ designat, metiri potest, nisi in altera formarum $mp+1$, $mp-1$ contineatur et vice versa omnes primi in his formis comprehensi formulae V erunt divisores.⁴

Quoties casus quartus locum habet, formula V duorum factorum rationalium productum esse invenitur, in quorum indolem iam profundius est inquirendum, ut decidatur, utrius eorum primus formulam metiens sit divisor.

Constat e theoria divisionis circuli, quae illi GATSS debetur, expressionem $4 \frac{t^p - u^p}{t - u}$, quoties p sit primus formae $4n+3$, redigi posse sub formam $R^2 + pS^2$, ubi R et S sunt functiones racionales integrae ipsius x . Formula $4 \frac{t^p - u^p}{t - u}$ manifesto est functio symmetrica ipsorum t et u , atque e demonstratione, qua vir summus theorema modo memoratum inuivit, facillime deducitur, R esse functionem, quae valorem oppositum nanciscitur, ipsis t et u inter se mutatis. Cum S sit functio symmetrica gradus $\frac{p-1}{2}$, erit summa plurium aggregatorum huius formae:

$$at^m u^{k-m} + at^{k-m} u^m,$$

ubi $k = \frac{p-1}{2}$ et $m < \frac{k}{2}$ supponere licet: tale aggregatum etiam hoc modo exhiberi potest:

$$at^m u^m (t^{k-2m} + u^{k-2m}).$$

Quodsi in hac expressione loco ipsorum t et u resp. $x + \sqrt{-p}$ et $x - \sqrt{-p}$ substituuntur, $t^m u^m$ obtinebit valorem $(x^2 + p)^m$, qui est functio par ipsius x (quo verbo brevitatis causa functionem designamus, in qua singuli exponentes sunt numeri pares). Alter factor $t^{k-2m} + u^{k-2m}$, cum exponens $k-2m$ sit impar, per eandem substitutionem mutabitur in functionem integram imparem ipsius x , id est, in functionem, in qua singuli exponentes sunt numeri impares. Aggregati illius valor post substitutionem erit igitur functio impar ipsius x .

Quoniam ea, quae modo diximus, valent de quovis aggregatorum, e quibus constat S , sequitur, S per eandem substitutionem mutatum iri in func-

tionem impari ipsius x . Hanc functionem, cuius coefficientes singulos pares esse facillime perspicitur, per $2S'$ designabimus.

Simili modo invenitur, formulam R , si loco ipsorum t et u resp. $x + \sqrt{-p}$ et $x - \sqrt{-p}$ substituatur, nacturam esse valorem, e duobus factoribus constantem, quorum prior est $\sqrt{-p}$, posterior functio rationalis par ipsius x . Posteriorem si per $2R'$ denotamus, $2R'\sqrt{-p}$ erit valor, quem R per substitutionem obtinet.

Si iam in formula $R^2 + pS^2$ loco ipsorum R et S resp. $2R'\sqrt{-p}$ et $2S'$ substituuntur, prodibit idem valor, quem nanciscitur $4 \frac{t^p - u^p}{t - u}$, loco ipsorum t et u resp. $x + \sqrt{-p}$ et $x - \sqrt{-p}$ substitutis. Habemus igitur:

$$2 \frac{(x + \sqrt{-p})^p - (x - \sqrt{-p})^p}{\sqrt{-p}} = 4pS'^2 - 4pR'^2,$$

et cum etiam sit:

$$V = \frac{(x + \sqrt{-p})^p - (x - \sqrt{-p})^p}{2\sqrt{-p}},$$

concluditur esse:

$$V = p(S' + R')(S' - R').$$

Demonstratum est igitur, formulam $\frac{V}{p}$ in duos factores rationales decomponi posse, quoties $b = -p$ et primus p sit formae $4u + 3$.

Cum R' sit functio par, S' autem functio impar ipsius x , manifestum est, signo ipsius x mutato, factorem priorem $S' + R'$ transiturum esse in $R' - S'$, id est, in posteriorem negative sumptum et vice versa posteriorem $S' - R'$, eadem mutatione perfecta, fore $-S' - R'$, id est, priori negative sumpto aequalem.

His ita stabilitis, sit k primus formulae V divisor et a valor ipsi x tribuendus, ut V per k fiat divisibilis. Iam dico, $R' + S'$ per k fore divisibilem, si x valorem idoneum obtineat. Cum enim k metiatur formulam $V = p(R' + S')(R' - S')$, ubi $x = a$ supponitur, aut $R' + S'$ aut $R' - S'$ per k erit divisibilis.

Si casus prior locum habet, a erit valor quaesitus; sin posterior, sequitur e praecedentibus $R' + S'$ per k fore divisibilem, si x ipsi $-a$ aequetur; hoc igitur casu valor idoneus erit $-a$.

Simili modo demonstratur, valorem ipsius x ita assumi posse, ut $R' - S'$ per k fiat divisibilis.

Quis igitur primus formulam V metiens erit divisor utriusque factorum $R' + S'$, $R' - S'$, ubi vix est mouendum, hos factores non pro eodem valore

ipsius x per k fore divisibiles, sed pro valoribus oppositis, id est, pro valoribus signo tantum discrepantibus.

Ut praecedentia exemplis nonnullis illustrentur, ponamus primo $p = 7$.

Factores ipsius V hoc casu inveniuntur esse:

$$x^3 - 7x^2 + 7x + 7, \quad x^3 + 7x^2 + 7x - 7,$$

qui manifesto respectu divisorum inter se non sunt diversi. Divisores primi harum formularum omnes in forma $7n \pm 1$ continentur, et vice versa quivis primus in hac forma comprehensus formularum erit divisor.

Sit secundo $p = 11$. Factores quinti gradus, quorum productum hoc casu est V , sunt hi:

$$x^5 + 11x^4 - 2 \cdot 11 \cdot x^3 - 2 \cdot 11^2 \cdot x^2 - 3 \cdot 11^2 \cdot x - 11^2, \quad x^5 - 11x^4 - 2 \cdot 11 \cdot x^3 + 2 \cdot 11^2 \cdot x^2 - 3 \cdot 11^2 \cdot x + 11^2,$$

quarum formularum neutra per primum erit divisibilis, nisi in forma $11n \pm 1$ contineatur, et vice versa quivis primus etc.

Hucusque supposuimus, numerum n in formulis (1) esse primum impari. Considerabimus iam casum, ubi n numeri 2 est potestas. Theoremata ad hunc casum pertinentia non ad formulam V , sed ad formulam U sunt referenda. — Numerum n in sequentibus per a designabimus, et k erit primus impar formulam U metiens. Iam duo casus sunt distinguendi, prout b ipsius k est residuum vel non-residuum quadraticum. Si b ipsius k est residuum, datur numerus μ ita comparatus, ut sit $\mu^2 \equiv b \pmod{k}$. Primus k , quem formulae U divisorem esse statuimus, eandem metietur, si μ^2 loco ipsius b substituerimus. Formula $2U$, quae, ut comparatio primae et secundae aequationum (1) docet, hoc quoque modo exhiberi potest:

$$2U = (x + \sqrt{b})^a + (x - \sqrt{b})^a,$$

substitutione modo indicata transibit in hanc $(x + \mu)^a + (x - \mu)^a$, quae manifesto per k divisibilis esse non potest, nisi k aut utrumque aut neutrum ipsorum $x + \mu$ et $x - \mu$ metiatur. Casum priorem locum habere non posse hoc modo demonstratur. Tum enim uterque numerorum:

$$\frac{1}{2}(x + \mu) + \frac{1}{2}(x - \mu), \quad \frac{1}{2}(x + \mu) - \frac{1}{2}(x - \mu),$$

seu uterque ipsorum x et μ per k esset divisibilis et quoniam est $b \equiv \mu^2 \pmod{k}$, k metiretur quoque ipsum b contra suppositionem, valores ipsi x tribuendos ad ipsum b esse primos.

Cum neuter ipsorum $x + \mu$, $x - \mu$ per k sit divisibilis, assignari potest numerus y huic congruentiae satisfaciens:

$$(x+\mu)y \equiv x-\mu \pmod{k}.$$

Quodsi iam in formula $2U$ loco ipsius $x-\mu$ valorem secundum mod. k congruum $y(x+\mu)$ substituerimus, obtinebimus hanc expressionem per k divisibilem $(x+\mu)^n(y^n+1)$. cuius factorem y^n+1 igitur primus k metiri debet, unde ope theorematum II concluditur, k esse formae $2m\alpha+1$. Habemus itaque theoremata:

„Omnes primi, quorum residuum est b , formulam U , in qua $n = \alpha$ est potestas numeri 2, metientes continentur in forma $2m\alpha+1$.“

Haec propositio etiam inversa valet et simili modo demonstrari potest.

Progredimur ad considerationem primorum, quorum non-residuum quadraticum est b et de quibus hoc theoremata valet:

„Si primus, cuius non-residuum est b , est formae $2m\alpha-1$, formulae U erit divisor, et vice versa nullus primus, cuius non-residuum est b , formulam metitur, nisi in forma $2m\alpha-1$ contineatur.“

Demonstrationem partis prioris huius theorematum, cum iis, quae supra exposuimus, satis sit similis, lectori evolvendam relinquimus. Posterioris autem demonstrationem, quae nova artificia requirit, fusius explicabimus. Sit k primus, cuius non-residuum est b , formulam U pro valore determinato ipsius x metiens, demonstrandum est nobis, k esse formae $2m\alpha-1$, seu $k+1$ per 2α esse divisibilem. Ponamus $k+1$ per 2α non esse divisibilem, et quid inde sequatur, videamus. Si per β summam potestatem numeri 2 ipsum $k+1$ metientem designamus, $\frac{k+1}{\beta}$ erit numerus impar et $\frac{2\alpha}{\beta}$ vel 2 vel potestas ipsius 2. Numeri $\frac{k+1}{\beta} \cdot \frac{2\alpha}{\beta}$ igitur divisorem communem non habent, unde sequitur, numeros integros positivos assignari posse ita comparatos, ut sit:

$$g \frac{k+1}{\beta} - \frac{2\alpha}{\beta} h = 1,$$

quae aequatio hoc quoque modo exhiberi potest: $g(k+1) - 2h\alpha = \beta$.

Supra vidimus, N in aequatione $M+N\sqrt{b} = (x+\sqrt{b})^{k+1}$ pro quovis valore ipsius x per k esse divisibilem. Expressionem $M+N\sqrt{b}$ ad potestatem g elevatam si per $M'+N'\sqrt{b}$ designamus, N' per N ideoque per k divisibilis erit, M' autem per k non divisibilem esse sequitur ex eo, quod $M'+N'\sqrt{b}$ manifesto est potestas ipsius $x+\sqrt{b}$, quam ob rem M' et N' divisorem communem imparem habere non possunt.

Habemus aequationem:

$$(x+\sqrt{b})^g = U+V\sqrt{b},$$

in qua, cum U per k sit divisibilis, formula V non erit, quippe quae ad formulam U est prima. Ex aequatione praecedenti deducitur haec:

$$(x+\sqrt{b})^{2a} = U^2 + bV^2 + 2UV\sqrt{b}$$

sen, quod est idem, si brevitatis causa ponimus $U^2 + bV^2 = P$, $2UV = Q$:

$$(x+\sqrt{b})^{2a} = P + Q\sqrt{b}.$$

Cum k ipsum b non metiatur, et U ipsius k sit multipulum, V autem non sit, concluditur, k ipsius Q esse divisorem, ipsius P autem non esse.

Iam si ponimus:

$$(P + Q\sqrt{b})^k = P' + Q'\sqrt{b},$$

ut supra demonstrari poterit, Q' ipsius k fore multipulum, P' autem non fore. —

E comparatione aequationum:

$$(x+\sqrt{b})^{a(k+1)} = M' + N'\sqrt{b}, \quad (x+\sqrt{b})^{2ka} = P' + Q'\sqrt{b}, \quad g(k+1) - 2ka = \beta,$$

deducitur haec:

$$M' + N'\sqrt{b} = (P' + Q'\sqrt{b})(x + \sqrt{b})^\beta,$$

quae, si brevitatis causa ponimus $(x + \sqrt{b})^\beta = R + S\sqrt{b}$, hoc quoque modo exhiberi potest:

$$M' + N'\sqrt{b} = (P' + Q'\sqrt{b})(R + S\sqrt{b}).$$

Concluditur inde, multiplicando et partes rationales et coefficientes ipsius \sqrt{b} separatim aequando, esse:

$$M' = P'R + bQ'S, \quad N' = P'S + Q'R.$$

Cum Q' et N' ipsius k sint multipla, k autem expressionem P' non metiatur, manifesto posterior aequationum praecedentium locum habere non potest, nisi S per k sit divisibilis.

Habemus aequationes:

$$(x+\sqrt{b})^a = U + V\sqrt{b}, \quad (x+\sqrt{b})^g = R + S\sqrt{b},$$

quarum comparatio hanc novam suppeditat:

$$U + V\sqrt{b} = (R + S\sqrt{b})^{\frac{a}{g}}.$$

ubi $\frac{a}{g}$ est integer, quia $\frac{2a}{g}$ est vel 2 vel potestas ipsius 2. Sequitur ex aequatione praecedenti, in qua exponens $\frac{a}{g}$ est integer, V per S esse divisibilem; et cum k , ut supra vidimus, formulam S metiatur, concludendum est, k esse divisorem formulae V , quod est contra ea, quae supra stabilivimus. Demonstravimus enim, formulas U et V divisorem communem imparem habere non posse, unde sequitur, primum k , quem formulae U divisorem esse statuimus, formulam V metiri non posse. Probatum est igitur, suppositionem, a qua pro-

fecti sumus, constare non posse, sed $k+1$ re vera per $2a$ esse divisibilem seu k esse formae $2ma-1$.

Ecce quaedam exempla ad theoremata modo demonstrata referenda.

Sit $a = 4$, quo casu U invenitur $x^4 + 6bx^2 + b^2$, quae formula per nullum primum, cuius residuum quadraticum est b , erit divisibilis, nisi in forma $8m+1$ contentum, et per nullum primum, cuius non-residuum est b , nisi in forma $8m-1$ sit inclusus.

Ponamus $b = -3$, qua suppositione U erit $x^4 - 18x^2 + 9$. Constat autem e doctrina de residuis quadraticis, primos, quorum residuum sit -3 , esse formae $3m+1$, primos, quorum non-residuum -3 , esse formae $3m-1$. Quae si cum praecedentibus comparaveris, invenies: „formulam $x^4 - 18x^2 + 9$ per nullum primum esse divisibilem, nisi in altera formarum $24m \pm 1$ contineatur, et vice versa, quemvis primum etc.“

Aliud exemplum praebent suppositiones $a = 8$, $b = 5$, quo casu valor formulae U erit $x^8 + 140x^6 + 1750x^4 + 3500x^2 + 625$, cuius expressionis divisores primi erunt formae $16m+1$ vel formae $16m-1$, prout 5 eorum est residuum vel non-residuum quadraticum. Quod si cum propositione nota: „primos, quorum residuum sit 5 , esse formae $5m \pm 1$, primos autem, quorum non-residuum sit 5 , esse formae $5m \pm 2$ “ rite iunxeris, prodibit hoc theorema:

„Primi formulam $x^8 + 140x^6 + 1750x^4 + 3500x^2 + 625$ metientes continentur in formis $80m+1$, 47 , 49 , 63 , et vice versa quivis primus in aliqua harum formarum comprehensus formulae erit divisor.“

RECHERCHES SUR LES DIVISEURS PREMIERS
D'UNE CLASSE DE FORMULES DU QUATRIÈME
DEGRÉ.

PAR

M. G. LEJEUNE DIRICHLET,
PROF. DE MATH. A BRESLAU

Crelle, Journal für die reine und angewandte Mathematik, Bd. 3 p. 35—69.

RECHERCHES SUR LES DIVISEURS PREMIERS D'UNE CLASSE DE FORMULES DU QUATRIÈME DEGRÉ.

1^{er} M é m o i r e.

On trouve, dans les annonces littéraires de Gottingue (11 avril 1825), l'extrait d'un mémoire d'analyse indéterminée que M. GAUSS a présenté à la Société Royale des Sciences de cette ville, mais qui n'a pas encore été imprimé. Ce mémoire est le premier d'une suite de mémoires que l'illustre auteur des *Disquisitiones arithmeticae* se propose de donner sur la théorie des résidus biquadratiques, et a pour objet de déterminer les caractères distinctifs des nombres premiers diviseurs de la formule $x^4 - 2$. L'auteur y établit deux théorèmes extrêmement élégants qui peuvent servir à décider, si un nombre premier, diviseur de $x^2 - 2$, divise ou ne divise pas la formule précédente. Ayant eu connaissance, dans le courant de l'année qui vient de finir, de l'extrait cité qui ne contient que les énoncés des deux théorèmes dont il vient d'être question, et de quelques propositions auxiliaires, j'eus le désir de démontrer de mon côté les beaux théorèmes découverts par M. GAUSS. Les recherches que je fis dans cette vue me firent trouver une démonstration fondée sur des considérations extrêmement simples et probablement tout-à-fait différente de celle de M. GAUSS, qui paraît exiger des recherches préliminaires très délicates et assez étendues. J'appliquai ensuite des considérations analogues à d'autres questions et particulièrement à la recherche des propriétés qui distinguent les diviseurs premiers de la formule $\alpha x^4 + \beta x^2 + \gamma$; et je parvins ainsi à un grand nombre de théorèmes intéressants. L'exposition rapide d'une partie des résultats auxquels ces recherches m'ont conduit, est l'objet du présent mémoire. Je commence par poser quelques définitions et par énoncer quelques théorèmes très faciles à établir et sur lesquels nous aurons à nous appuyer dans la suite.

1.

„Si l'on peut attribuer à l'indéterminée x une valeur telle que $x^4 - A$ devienne divisible par B , A sera dit résidu biquadratique par rapport à B .“

Il est facile de voir que, si un nombre A est résidu biquadratique par rapport à un nombre B , ou en d'autres termes, si B est diviseur de $x^4 - A$, chaque facteur premier de B sera pareillement diviseur de $x^4 - A$, et réciproquement, que si cette condition a lieu par rapport à tout facteur premier du nombre B , B sera lui-même diviseur de $x^4 - A$. On peut donc se borner, lorsqu'il s'agit d'assigner tous les nombres qui divisent la formule $x^4 - A$, à ne considérer que les nombres premiers.

Il n'est pas moins évident que, pour qu'un nombre divise la formule $x^4 - A$, il est nécessaire que ce nombre soit diviseur de $x^2 - A$. Il n'y a donc à examiner que les nombres premiers diviseurs de cette dernière formule, c'est-à-dire les nombres premiers par rapport auxquels A est résidu quadratique. On peut ajouter que, relativement à ceux de ces derniers qui sont de la forme $4n + 3$, la question ne présente aucune difficulté; car on s'assure par un raisonnement très simple que tout nombre premier $4n + 3$, diviseur de $x^2 - A$, divise aussi la formule $x^4 - A$.

Soit p un nombre premier $4n + 1$, diviseur de $x^2 - A$, A désignant un nombre positif ou négatif, non-divisible par p ; on a, comme l'on sait, $A^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. On conclut de là, $A^{\frac{p-1}{4}} \equiv \pm 1 \pmod{p}$ et l'on prouve facilement que le signe supérieur ou inférieur aura lieu, selon que p divise ou ne divise pas la formule $x^4 - A$. On peut donc énoncer ce théorème:

„ A désignant un nombre résidu quadratique par rapport au nombre premier $p = 4n + 1$, on aura $A^{\frac{p-1}{4}} \equiv 1$ ou $A^{\frac{p-1}{4}} \equiv -1 \pmod{p}$. Dans le premier cas, A sera résidu biquadratique par rapport à p , dans le second, A sera non-résidu biquadratique par rapport à p .“

Si l'on applique ce théorème au cas où $A = -1$, on trouvera que -1 est résidu biquadratique par rapport aux nombres premiers $8n + 1$, et au contraire non-résidu relativement à ceux de la forme $8n + 5$. Du théorème précédent on déduit facilement cet autre, dans l'énoncé duquel on suppose, comme dans tout ce qui suivra, que p soit un nombre premier $4n + 1$, et que A et A' désignent des nombres non-divisibles par p et qui sont l'un et l'autre des résidus quadratiques par rapport à p .

„Si les nombres A et A' sont tous les deux des résidus biquadratiques ou tous les deux des non-résidus biquadratiques par rapport à p , le produit AA' sera résidu biquadratique par rapport à p ; si, au contraire, l'un des nombres A et A' est résidu, l'autre non-résidu biquadratique relativement à p , AA' sera non-résidu biquadratique par rapport à p .“

En faisant $A' = -1$, et en ayant égard à ce qui précède, on verra que, si p est de la forme $8n+1$, A sera en même temps que $-A$ résidu ou non-résidu biquadratique, et qu'au contraire, si p est de la forme $8n+5$, l'un des nombres A et $-A$ sera résidu, l'autre non-résidu biquadratique par rapport à p .

2.

Après avoir établi ces préliminaires, nous allons nous occuper de la recherche des caractères qui distinguent les diviseurs premiers de la formule $x^2 - 2$. On sait que les diviseurs premiers de $x^2 - 2$ sont de l'une de ces deux formes: $8n+1$, $8n+7$, et que réciproquement tout nombre premier de l'une de ces formes divise la formule $x^2 - 2$. D'après ce que nous avons dit dans le paragraphe précédent, nous n'avons pas besoin d'avoir égard à la dernière de ces deux formes, et il suffira de considérer les nombres premiers $8n+1$. Soit p un nombre premier de cette espèce, et posons, comme il est permis de le faire, $p = t^2 + 2u^2$, où u sera pair, t impair. Faisons $u = 2^r k k' k'' \dots$, 2^r étant la puissance la plus élevée de 2 qui divise u , et k, k', k'', \dots désignant des nombres premiers impairs, dont plusieurs peuvent être égaux entre eux. L'équation $t^2 + 2u^2 = p$ donne immédiatement $t^2 \equiv p \pmod{k}$. Le nombre p est donc résidu quadratique par rapport à k , ce que nous écrirons ainsi:

$\left(\frac{p}{k}\right) = 1$, en adoptant la notation employée par M. LEGENDRE. On se rappelle que, si c désigne un nombre premier et M un nombre quelconque, non divisible par c , cet illustre géomètre se sert du signe $\left(\frac{M}{c}\right)$, pour désigner le reste

que l'on obtient, en divisant par c la puissance $M^{\frac{c-1}{2}}$, reste que l'on sait être égal à 1 ou -1 , selon que M est ou n'est pas résidu quadratique par rapport à c . En appliquant à la relation $\left(\frac{p}{k}\right) = 1$, le théorème connu sous le nom de loi de réciprocité (*theoremata fundamentale* de M. GAUSS), on aura, p étant

de la forme $4n+1$, $\left(\frac{k}{p}\right) = 1$. On trouve de la même manière:

$$\left(\frac{k'}{p}\right) = 1, \quad \left(\frac{k''}{p}\right) = 1, \quad \text{etc.}$$

D'un autre côté, comme p est de la forme $8n+1$, on a aussi $\left(\frac{2}{p}\right) = 1$, et par conséquent $\left(\frac{2^v}{p}\right) = 1$. Multipliant cette dernière relation par toutes les précédentes, il viendra:

$$\left(\frac{2^v k k' k'' \dots}{p}\right) = \left(\frac{u}{p}\right) = 1.$$

Considérons maintenant les facteurs simples du nombre impair t , que nous partagerons en deux classes. La première classe comprendra les diviseurs premiers de l'une de ces deux formes: $8n+1$, $8n+7$, et les nombres qui en font partie seront désignés par g , g' , g'' , ...; la seconde classe se composera de nombres h , h' , h'' , ...; contenus dans ces deux formes: $8n+3$, $8n+5$. On a d'abord:

$$t = gg'g'' \dots \times hh'h'' \dots,$$

et l'on conclura ensuite de l'équation $p = t^2 + 2u^2$:

$$\left(\frac{2p}{g}\right) = 1, \quad \left(\frac{2p}{g'}\right) = 1, \quad \left(\frac{2p}{g''}\right) = 1, \quad \text{etc.}$$

$$\left(\frac{2p}{h}\right) = 1, \quad \left(\frac{2p}{h'}\right) = 1, \quad \left(\frac{2p}{h''}\right) = 1, \quad \text{etc.}$$

D'un autre côté, on a en vertu de théorèmes connus:

$$\left(\frac{2}{g}\right) = 1, \quad \left(\frac{2}{g'}\right) = 1, \quad \left(\frac{2}{g''}\right) = 1, \quad \text{etc.}$$

$$\left(\frac{2}{h}\right) = -1, \quad \left(\frac{2}{h'}\right) = -1, \quad \left(\frac{2}{h''}\right) = -1, \quad \text{etc.}$$

Si l'on compare maintenant ces relations aux précédentes, on trouvera:

$$\left(\frac{p}{g}\right) = 1, \quad \left(\frac{p}{g'}\right) = 1, \quad \left(\frac{p}{g''}\right) = 1, \quad \text{etc.}$$

$$\left(\frac{p}{h}\right) = -1, \quad \left(\frac{p}{h'}\right) = -1, \quad \left(\frac{p}{h''}\right) = -1, \quad \text{etc.}$$

L'application de la loi de réciprocité à ces dernières relations donnera celles-ci:

$$\left(\frac{g}{p}\right) = 1, \quad \left(\frac{g'}{p}\right) = 1, \quad \left(\frac{g''}{p}\right) = 1, \quad \text{etc.}$$

$$\left(\frac{h}{p}\right) = -1, \quad \left(\frac{h'}{p}\right) = -1, \quad \left(\frac{h''}{p}\right) = -1, \quad \text{etc.}$$

d'où il suit, en multipliant :

$$\left(\frac{gg'g'' \dots \times hh'h'' \dots}{p} \right) = \left(\frac{t}{p} \right) = \pm 1,$$

où il faudra prendre le signe supérieur ou inférieur, selon que les nombres h, h', h'', \dots sont en nombre pair ou impair. Or, il est facile de voir, par l'équation $t = gg'g'' \dots \times hh'h'' \dots$, que le premier cas aura lieu, lorsque t est de l'une de ces formes: $8n+1, 8n+7$, le second, lorsque t est contenu dans l'une de celles-ci: $8n+3, 8n+5$. On a donc :

$$\begin{aligned} \left(\frac{t}{p} \right) &= 1, & \text{lorsque } t &= 8n+1 \text{ ou } 8n+7, \\ \left(\frac{t}{p} \right) &= -1, & \text{lorsque } t &= 8n+3 \text{ ou } 8n+5. \end{aligned}$$

Reprenons l'équation $t^2 + 2u^2 = p$ et mettons-la sous la forme d'une congruence :

$$t^2 \equiv -2u^2 \pmod{p}.$$

En élevant les deux membres à la puissance $\frac{p-1}{4}$, on aura $\left(\frac{p-1}{4} \right.$ étant pair) :

$$t^{\frac{p-1}{2}} \equiv 2^{\frac{p-1}{4}} u^{\frac{p-1}{2}} \pmod{p}.$$

ou, ce qui revient au même, ayant prouvé que $\left(\frac{u}{p} \right) = 1$:

$$t^{\frac{p-1}{2}} \equiv 2^{\frac{p-1}{4}} \pmod{p}.$$

On voit donc que ± 2 (on peut mettre le double signe attendu que $p = 8n+1$) est ou n'est pas résidu biquadratique par rapport à p , selon que l'on a $\left(\frac{t}{p} \right) = 1$ ou $\left(\frac{t}{p} \right) = -1$. En comparant ce résultat à ce qui précède, on aura ce théorème :

« p désignant un nombre premier $8n+1$, si l'on fait $p = t^2 + 2u^2$, je dis que ± 2 sera ou ne sera pas résidu biquadratique par rapport à p , selon que t est de l'une de ces formes: $8n+1, 8n+7$ ou de l'une de celles-ci: $8n+3, 8n+5$. »

C'est le premier des deux théorèmes de M. GAUSS, dont il a été question dans le préambule de ce mémoire. Le second de ces théorèmes est relatif à la décomposition du nombre p en deux carrés, et peut être facilement déduit de celui qui vient d'être établi.

Faisons $p = \varphi^2 + \psi^2$ (où ψ est supposé divisible par 4) et égalons cette valeur de p à celle que nous venons de considérer.

Nous aurons ainsi:

$$p = t^2 + 2u^2 = g^2 + \psi^2,$$

et en transposant:

$$t^2 - \psi^2 = (t + \psi)(t - \psi) = g^2 - 2u^2.$$

Comme g est impair, le plus grand diviseur commun de g et u sera impair: désignons-le par m et faisons $g = mg'$, $u = mu'$. La substitution de ces valeurs dans l'équation précédente la changera en celle-ci:

$$(t + \psi)(t - \psi) = m^2(g'^2 - 2u'^2).$$

On voit que le nombre impair $t + \psi$ est composé de deux facteurs E et K , dont le premier divise m^2 , le second $g'^2 - 2u'^2$, et qu'il en est de même de $t - \psi$ dont nous désignerons les facteurs par F et L , L pouvant être négatif. Nous avons donc les équations:

$$\begin{aligned} t + \psi &= EK, & t - \psi &= FL, \\ m^2 &= EF, & g'^2 - 2u'^2 &= KL. \end{aligned}$$

Il est facile de s'assurer que les nombres E et F sont premiers entre eux. En effet, soit δ un diviseur premier de E , et supposons que δ divise en même temps F . Le nombre δ serait diviseur commun de $t + \psi$ et $t - \psi$, et diviserait par conséquent le nombre t , qui est la demi-somme des précédents. D'un autre côté, de ce que δ est diviseur premier de E , il suit successivement, en ayant égard aux équations $EF = m^2$, $u = mu'$, que m^2 , m et u sont multiples de δ . Les nombres t et u auraient donc le diviseur commun δ , et $p = t^2 + 2u^2$ ne serait pas un nombre premier.

Le produit des nombres E et F , qui sont premiers entre eux, étant un carré, chacun d'eux est aussi un carré. Faisons $E = e^2$, et nous aurons $t + \psi = e^2K$. Le carré impair e^2 est de la forme $8n + 1$, et K , comme diviseur impair de $g'^2 + 2u'^2$ (où g' et u' sont premiers entre eux), de l'une de celles-ci: $8n + 1$, $8n + 7$. Le nombre $t + \psi$ sera donc lui-même de l'une des formes $8n + 1$, $8n + 7$. Le nombre ψ que nous savons être divisible par 4, sera de la forme $8n$ ou de celle-ci: $8n + 4$. Il suit, de ce qui précède, que, dans le premier cas, t sera de l'une de ces deux formes: $8n + 1$, $8n + 7$, dans le second de l'une de celles-ci: $8n + 3$, $8n + 5$. En comparant ce résultat au théorème précédent, on aura cet autre théorème:

„ p désignant un nombre premier $8n + 1$, et ayant fait $p = g^2 + \psi^2$ (où ψ est supposé divisible par 4), ± 2 sera ou ne sera pas résidu biquadratique par rapport à p , selon que ψ est de la forme $8n$ ou de celle-ci: $8n + 4$.”

Il y a un troisième théorème propre à décider si ± 2 est ou n'est pas résidu biquadratique relativement à un nombre premier $p = 8n + 1$, et qui peut s'énoncer comme il suit :

„Ayant fait d'une manière quelconque $p = t^2 - 2u^2$, ± 2 sera ou ne sera pas résidu biquadratique par rapport à p , selon que t est de l'une des formes $8n + 1$, $8n + 3$, ou de l'une de celles-ci : $8n + 5$, $8n + 7$.“

Nous ne nous arrêterons pas à démontrer ce théorème que l'on peut établir d'une manière directe et par des considérations analogues à celles sur lesquelles est fondée la démonstration du premier des deux théorèmes précédents. On peut aussi le déduire de chacun des précédents à-peu-près comme on vient de passer du premier au second.

3.

Nous allons maintenant passer à des considérations plus générales. Soit b un nombre premier $4n + 3$, p un nombre premier $4n + 1$ susceptible d'être mis sous la forme $t^2 - bu^2$, et proposons-nous de décider si $-b$ est ou n'est pas résidu biquadratique par rapport à p . Il est facile de voir que, si p peut être mis sous la forme $t^2 - bu^2$, on peut toujours le faire de manière que u soit pair, et par conséquent t impair³⁾. Faisons donc $p = t^2 - bu^2$, et posons $u = 2^r k k' k'' \dots$, k, k', k'', \dots étant les facteurs impairs simples de u . On conclut immédiatement de l'équation précédente :

$$\left(\frac{p}{k}\right) = 1, \quad \left(\frac{p}{k'}\right) = 1, \quad \left(\frac{p}{k''}\right) = 1, \quad \text{etc.}$$

L'application de la loi de réciprocité donne ensuite, p étant de la forme $4n + 1$:

$$\left(\frac{k}{p}\right) = 1, \quad \left(\frac{k'}{p}\right) = 1, \quad \left(\frac{k''}{p}\right) = 1, \quad \text{etc.}$$

Multipliant ces relations entre elles et avec la relation identique $\left(\frac{2^r}{p}\right) = \left(\frac{2^r}{p}\right)$.

³⁾ Pour prouver que cela est toujours possible, nous allons faire voir que, si l'on a $t^2 - bu^2 = p$, t étant pair, il est facile de déduire des valeurs de t et de u , d'autres nombres t' (impair) et u' qui satisfassent également à l'équation $t'^2 - bu'^2 = p$. Soient r et s les moindres nombres tels que $r^2 - bs^2 = 1$, je dis que r sera pair. En effet, on sait que, si b désigne un nombre premier $4n + 3$, l'équation $q^2 - bq^2 = \pm 2$ est toujours possible, et que, q et σ étant supposés les plus petits nombres qui y satisfont, on a $r = b\sigma^2 + 1$, $s = q\sigma$ (*Théorie des Nombres*, no. 44. 45). Il suit de là et de ce que les nombres q et σ sont évidemment impairs l'un et l'autre, que r est un nombre pair. Cela posé, si l'on multiplie entre elles les équations $r^2 - bs^2 = 1$, $t^2 - bu^2 = p$, il viendra $(rt \pm bsu)^2 - b(ru \pm st)^2 = p$, et l'on verra facilement que $rt \pm bsu$ est un nombre impair.

on aura ce résultat :

$$(\alpha) \quad \left(\frac{a}{p}\right) = \left(\frac{2^r}{p}\right).$$

Décomposons actuellement le nombre impair t en ses facteurs simples et partageons ces facteurs en deux classes. Ceux de la première classe seront désignés par g, g', g'', \dots et sont tels que :

$$(\beta) \quad \left(\frac{-b}{g}\right) = 1, \quad \left(\frac{-b}{g'}\right) = 1, \quad \left(\frac{-b}{g''}\right) = 1, \quad \text{etc.}$$

Quant à ceux qui forment la seconde classe et que nous désignerons par h, h', h'', \dots ils sont tels que :

$$(\beta') \quad \left(\frac{-b}{h}\right) = -1, \quad \left(\frac{-b}{h'}\right) = -1, \quad \left(\frac{-b}{h''}\right) = -1, \quad \text{etc.}$$

Le produit de tous ces nombres est égal à t , c'est-à-dire que :

$$t = gg'g''\dots \times hh'h''\dots$$

L'inspection de l'équation $t^2 - bu^2 = p$ donne ces résultats :

$$\begin{aligned} \left(\frac{-bp}{g}\right) &= 1, & \left(\frac{-bp}{g'}\right) &= 1, & \left(\frac{-bp}{g''}\right) &= 1, & \text{etc.} \\ \left(\frac{-bp}{h}\right) &= 1, & \left(\frac{-bp}{h'}\right) &= 1, & \left(\frac{-bp}{h''}\right) &= 1, & \text{etc.} \end{aligned}$$

La comparaison de ces relations avec les précédentes donnera ensuite :

$$\begin{aligned} \left(\frac{p}{g}\right) &= 1, & \left(\frac{p}{g'}\right) &= 1, & \left(\frac{p}{g''}\right) &= 1, & \text{etc.} \\ \left(\frac{p}{h}\right) &= -1, & \left(\frac{p}{h'}\right) &= -1, & \left(\frac{p}{h''}\right) &= -1, & \text{etc.} \end{aligned}$$

Appliquant maintenant la loi de réciprocité, il viendra :

$$\begin{aligned} \left(\frac{g}{p}\right) &= 1, & \left(\frac{g'}{p}\right) &= 1, & \left(\frac{g''}{p}\right) &= 1, & \text{etc.} \\ \left(\frac{h}{p}\right) &= -1, & \left(\frac{h'}{p}\right) &= -1, & \left(\frac{h''}{p}\right) &= -1, & \text{etc.} \end{aligned}$$

Multipliant ces relations entre elles, on aura :

$$\left(\frac{gg'g''\dots \times hh'h''}{p}\right) = \left(\frac{t}{p}\right) = \pm 1.$$

le signe supérieur ou inférieur ayant lieu, selon que les nombres h, h', h'', \dots sont en nombre pair ou impair. D'un autre côté, si l'on applique la loi de réciprocité aux relations (β) et (β') , il viendra, b étant de la forme $4n+3$:

$$\left(\frac{g}{b}\right) = 1, \quad \left(\frac{g'}{b}\right) = 1, \quad \left(\frac{g''}{b}\right) = 1, \quad \text{etc.}$$

$$\left(\frac{h}{b}\right) = -1, \quad \left(\frac{h'}{b}\right) = -1, \quad \left(\frac{h''}{b}\right) = -1, \quad \text{etc.}$$

égalités qui, étant multipliées entre elles, donneront celle-ci :

$$\left(\frac{gg'g'' \dots \times hh'h''}{b}\right) = \left(\frac{t}{b}\right) = \pm 1,$$

où il faut prendre le signe supérieur ou inférieur, selon que les nombres h , h' , h'' , ... sont en nombre pair ou impair.

La comparaison de ce résultat avec celui que nous avons obtenu, il n'y a qu'un instant, fait voir qu'on a toujours :

$$(y) \quad \left(\frac{t}{p}\right) = \left(\frac{t}{b}\right).$$

Reprenons maintenant l'équation $p = t^2 - hu^2$, et mettons-la sous la forme d'une congruence :

$$t^2 \equiv hu^2 \pmod{p}.$$

On tire de là, en élevant les deux membres à la puissance $\frac{p-1}{4}$:

$$t^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{4}} u^{\frac{p-1}{2}} \pmod{p}.$$

La formule (α), qui est celle-ci : $\left(\frac{u}{p}\right) = \left(\frac{2^\nu}{p}\right)$, 2^ν désignant la puissance la plus élevée qui divise u , peut être présentée d'une autre manière. Il faut pour cela distinguer deux cas, selon que p est de la forme $8n+1$ ou de celle-ci : $8n+5$.

Si p est un nombre premier $8n+1$, on a, comme on sait, $\left(\frac{2}{p}\right) = 1$, et par conséquent $\left(\frac{2^\nu}{p}\right) = 1$: la formule dont il s'agit se change donc dans ce cas en

celle-ci : $\left(\frac{u}{p}\right) = 1$. Si p est un nombre premier $8n+5$, le nombre ν est = 1 ; car si ν était plus grand que l'unité, u^2 serait divisible par 8, et $p = t^2 - hu^2$ serait de la forme $8n+1$. Comme d'ailleurs dans ce cas $\left(\frac{2}{p}\right) = -1$, la formule (α) se changera en celle-ci : $\left(\frac{u}{p}\right) = -1$. Les deux cas que nous venons

d'examiner sont compris dans la formule $\left(\frac{u}{p}\right) = (-1)^{\frac{\nu-1}{4}}$, qui équivaut à cette congruence : $u^{\frac{p-1}{2}} \equiv (-1)^{\frac{\nu-1}{4}} \pmod{p}$. En substituant la valeur qu'elle donne

pour u^{p-1} dans la congruence obtenue plus haut, on aura :

$$t^2 \equiv (-b)^{\frac{p-1}{4}} \pmod{p}.$$

résultat qui montre que $-b$ sera ou ne sera pas résidu biquadratique par rapport à p , selon que t est ou n'est pas résidu quadratique par rapport à p . Si l'on compare maintenant ce résultat avec celui qui est contenu dans la formule (7), on arrivera au théorème que nous allons énoncer :

„Désignons par b un nombre premier $4n+3$, et par p un nombre premier $4n+1$, susceptible d'être mis sous la forme t^2-bu^2 . Ayant fait $p = t^2-bu^2$ (où t est supposé impair), je dis que $-b$ sera ou ne sera pas résidu biquadratique par rapport à p , selon que t est ou n'est pas résidu quadratique par rapport à b .“

4.

Nous allons maintenant déduire de ce théorème un autre, au moyen duquel on peut décider plus promptement encore, si $-b$ est ou n'est pas résidu biquadratique par rapport à p . Conservons les notations précédentes et faisons $p = g^2 + \psi^2$ (où ψ est supposé pair). En égalant cette valeur de p à celle que nous avons considérée précédemment, on aura :

$$p = t^2 - bu^2 = g^2 + \psi^2,$$

et en transposant :

$$t^2 - \psi^2 = (t + \psi)(t - \psi) = g^2 + bu^2.$$

Il y a maintenant deux cas à distinguer, selon que g est ou n'est pas divisible par b . Nous commençons par l'examen du dernier de ces deux cas. Soit m le plus grand commun diviseur de g et u qui sera impair (g étant impair) et non-divisible par b , et posons $g = mg'$, $u = mu'$. La substitution de ces valeurs dans la dernière équation, la changera en celle-ci :

$$(t + \psi)(t - \psi) = m^2(g'^2 + bu'^2).$$

Il est évident, par cette équation, que $t + \psi$ est composé de deux facteurs E et K dont le premier divise m^2 , le second $g'^2 + bu'^2$, et qu'il en est de même de $t - \psi$. Désignant les facteurs de ce dernier nombre par F et L , nous aurons ces équations :

$$\begin{aligned} t + \psi &= EK, & t - \psi &= FL, \\ m^2 &= EF, & g'^2 + bu'^2 &= KL. \end{aligned}$$

Il est très facile de s'assurer que les nombres E et F sont premiers entre eux. En effet, soit δ un facteur simple quelconque de E (qui sera nécessairement impair, E étant lui-même impair) et supposons que δ divise aussi F . L'inspection des équations précédentes fait voir que δ serait, dans cette supposition, diviseur commun de $t+\psi$ et $t-\psi$, et diviserait par conséquent le nombre t , qui est la demi-somme des précédents. Mais on voit d'un autre côté que δ , comme diviseur premier de E , divise m^2 , et par conséquent m et n (n étant $= mu'$). Les nombres t et n auraient donc, dans cette supposition, le facteur commun δ , ce qui est absurde, $p = t^2 - bn^2$ étant un nombre premier. Il est donc prouvé que E et F ne sauraient avoir de diviseur commun, et comme le produit de ces nombres est un carré, chacun d'eux est pareillement un carré. On a donc :

$$\left(\frac{E}{b}\right) = 1, \quad \left(\frac{F}{b}\right) = 1.$$

Quant aux nombres K et L , ils sont de même tels qu'on ait :

$$\left(\frac{K}{b}\right) = 1, \quad \left(\frac{L}{b}\right) = 1.$$

En effet, on voit par la dernière équation (p. 74) que ces nombres divisent l'un et l'autre la formule $g'^2 + bu'^2$ (où g' et bu' sont premiers entre eux) et l'on sait par un théorème connu qui se déduit facilement de la loi de réciprocité (*Théorie des Nombres*, no. 197) que tout diviseur impair R d'une pareille formule est tel que $\left(\frac{R}{b}\right) = 1$. Multipliant la première des dernières relations par la troisième, la seconde par la quatrième, il viendra :

$$\left(\frac{EK}{b}\right) = 1, \quad \left(\frac{FL}{b}\right) = 1.$$

ou, ce qui est la même chose :

$$(\delta) \quad \left(\frac{t+\psi}{b}\right) = 1, \quad \left(\frac{t-\psi}{b}\right) = 1.$$

En examinant d'une manière semblable le cas de g divisible par b , on trouvera que, dans ce cas, l'un des nombres $t+\psi$ et $t-\psi$ est divisible par b , et que l'autre est, comme dans le cas dont nous venons de nous occuper, résidu quadratique par rapport à b , de sorte qu'en désignant par $t \pm \psi$ celui de ces nombres qui est divisible par b , on a :

$$(\delta') \quad t \pm \psi \equiv 0 \pmod{b}, \quad \left(\frac{t \mp \psi}{b}\right) = 1.$$

Il résulte du théorème énoncé à la fin du paragraphe précédent que, pour décider si $-b$ est ou n'est pas résidu biquadratique par rapport à p , tout se réduit à la question de savoir si t est ou n'est pas résidu quadratique par rapport à b . Nous pouvons maintenant faire voir, au moyen des résultats que nous venons d'obtenir, que cette dernière question peut être décidée sans connaître t , c'est-à-dire sans qu'il soit nécessaire de mettre p sous la forme $t^2 - bu^2$. Supposons d'abord g non-divisible par b . Les relations (8), qui ont lieu dans ce cas, peuvent être présentées de cette manière, en observant que b est un nombre premier $4n+3$:

$$\left(\frac{\psi+t}{b}\right) = 1, \quad \left(\frac{\psi-t}{b}\right) = -1.$$

On tire immédiatement de l'équation $p = t^2 - bu^2$: $t^2 \equiv p \pmod{b}$, résultat qui fait voir qu'en résolvant la congruence $z^2 \equiv p \pmod{b}$, et désignant par χ l'une de ses racines prise au hasard, on aura $t \equiv \chi$, ou $t \equiv -\chi \pmod{b}$. Dans le premier cas, on a:

$$\left(\frac{t}{b}\right) = \left(\frac{\chi}{b}\right), \quad \left(\frac{\chi+\psi}{b}\right) = 1,$$

car il est évident que les expressions $\left(\frac{t}{b}\right)$ et $\left(\frac{t+\psi}{b}\right)$ ne changent pas en mettant à la place de t un autre nombre χ qui ne diffère de t que par un multiple de b . En multipliant les dernières relations entre elles, il viendra:

$$\left(\frac{t}{b}\right) = \left(\frac{\chi(\chi+\psi)}{b}\right).$$

Considérons maintenant l'autre cas dans lequel $t \equiv -\chi \pmod{b}$. On aura alors:

$$\left(\frac{t}{b}\right) = -\left(\frac{\chi}{b}\right), \quad \left(\frac{\psi+\chi}{b}\right) = -1,$$

la dernière de ces relations résultant de la formule $\left(\frac{\psi-t}{b}\right) = -1$, si l'on met à la place de $-t$ le nombre χ qui n'en diffère que par un multiple de b . En multipliant les relations précédentes entre elles, on trouvera, comme plus haut:

$$\left(\frac{t}{b}\right) = \left(\frac{\chi(\chi+\psi)}{b}\right).$$

Nous sommes donc arrivés à ce résultat remarquable: Si g n'est pas divisible par b , on pourra décider très simplement si l'on a:

$$\left(\frac{t}{b}\right) = 1 \quad \text{ou} \quad \left(\frac{t}{b}\right) = -1.$$

Il suffira de chercher un nombre qui satisfasse à la congruence $x^2 \equiv p \pmod{b}$: ayant trouvé un pareil nombre x , on aura toujours:

$$\left(\frac{t}{b}\right) = \left(\frac{x(x+\psi)}{b}\right).$$

Venons maintenant au cas où q est divisible par b . Les relations (d') qui ont lieu alors, sont:

$$t \pm \psi \equiv 0 \pmod{b}, \quad \left(\frac{t \mp \psi}{b}\right) = 1.$$

On peut dans la dernière de ces relations ajouter à $t \mp \psi$ un multiple quelconque de b . Si l'on y ajoute le nombre $t \pm \psi$ qui, en vertu de la première, est divisible par b , il viendra $\left(\frac{2t}{b}\right) = 1$, résultat qui entraîne cet autre: $\left(\frac{t}{b}\right) = \left(\frac{2}{b}\right)$.

En combinant ce résultat avec un théorème connu, on verra que, dans le cas de q divisible par b , on a $\left(\frac{t}{b}\right) = 1$ ou $\left(\frac{t}{b}\right) = -1$, selon que t est de la forme $8n+7$ ou de celle-ci: $8n+3$.

En comparant ce qui vient d'être prouvé au théorème établi à la fin du dernier paragraphe, on verra qu'on peut décider, indépendamment de la connaissance du nombre t , si $-b$ est ou n'est pas résidu biquadratique par rapport à p . Le résultat auquel on parvient ainsi ne contenant plus aucune trace du nombre t , on est porté à croire qu'il ne suppose pas la possibilité de l'équation $t^2 - bu^2 = p$, d'où le nombre t tire son origine, et qu'il est généralement vrai pour toutes les valeurs de b et p , telles que $\left(\frac{b}{p}\right) = 1$. C'est en effet ce qui a lieu, comme on peut le prouver, en examinant, au lieu de l'équation $t^2 - bu^2 = p$, l'équation plus générale $t^2 \pm Mu^2 = p$, où M désigne le produit d'un nombre quelconque de nombres premiers différents, et en combinant ensuite les résultats de cet examen avec le théorème suivant, de la vérité duquel on ne saurait douter, mais dont la démonstration rigoureuse ne laisse pas que de présenter des difficultés:

« c désignant un nombre premier quelconque et p un nombre premier $4n+1$, tel que $\left(\frac{c}{p}\right) = 1$, on pourra toujours déterminer un nombre δ , composé de facteurs simples tous moindres que c et tel que l'équation $t^2 \pm c\delta u^2 = p$, soit résoluble.»

Quoi qu'il en soit, on peut remarquer que le théorème que nous allons énoncer est rigoureusement prouvé, par ce qui précède, pour toutes les valeurs

de b , telles que la formule $t^2 - bt^2$ n'ait que le seul diviseur quadratique $\pm(t^2 - bt^2)$. En jetant les yeux sur la première des tables ajoutées à la *Théorie des Nombres*, on voit que tous les nombres premiers $4n+3$, moindres que 136 (limite de la table) se trouvent dans ce cas, en exceptant le seul nombre 79. Il serait facile, en suivant la marche que nous venons d'indiquer, de prouver la vérité du théorème pour cette valeur ou pour toute autre valeur particulière de b , quel que soit p ; mais pour l'établir dans toute sa généralité, il faut d'abord prouver, comme nous l'avons déjà dit, qu'on peut toujours satisfaire à la condition que nous avons énoncée, il n'y a qu'un instant.

Théorème I.

b désignant un nombre premier $4n+3$, et p un nombre premier $4n+1$ tel que $\left(\frac{b}{p}\right) = 1$, si l'on fait $p = g^2 + \psi^2$ (où ψ est supposé pair) on aura cette règle pour décider si $-b$ est ou n'est pas résidu biquadratique par rapport à p : Si g est divisible par b , $-b$ sera ou ne sera pas résidu biquadratique, selon que b est de la forme $8n+7$ ou de celle-ci: $8n+3$. Si g n'est pas divisible par b , on cherchera un nombre x tel qu'on ait $x^2 \equiv p \pmod{b}$. Cela posé, $-b$ sera ou ne sera pas résidu biquadratique par rapport à p , selon que l'on a $\left(\frac{x(x+\psi)}{b}\right) = 1$ ou $\left(\frac{x(x+\psi)}{b}\right) = -1$.

En faisant successivement $b = 3$, $b = 7$ etc., on obtiendra les théorèmes particuliers suivants qui sont analogues au second des théorèmes de M. GAUSS et que l'on doit regarder comme rigoureusement prouvés par les considérations que nous avons exposées dans ce paragraphe et dans le précédent.

p désignant un nombre premier $12n+1$, si l'on fait $p = g^2 + \psi^2$ (où ψ est supposé pair) l'un des nombres g et ψ sera nécessairement divisible par 3. Cela posé, je dis que -3 sera ou ne sera pas résidu biquadratique par rapport à p , selon que c'est ψ ou g qui est divisible par 3.

p désignant un nombre premier de l'une de ces formes: $28n+1$, $28n+9$, $28n+25$, si l'on fait $p = g^2 + \psi^2$, je dis que -7 sera résidu biquadratique par rapport à p , si l'un des nombres g et ψ est divisible par 7, et que -7 sera non-résidu biquadratique par rapport à p , si ni l'un ni l'autre de ces nombres n'est divisible par 7.

etc.

5.

Désignons par a un nombre premier $4n+1$, et par p un nombre premier également $4n+1$, et de plus susceptible d'être mis sous la forme t^2-au^2 . Nous pouvons donc faire $p=t^2-au^2$ où le nombre t , comme il est facile de le voir, est nécessairement impair. On trouvera, comme dans le paragraphe 3, que, si l'on désigne par 2^r la puissance la plus élevée de 2 qui divise u , on a $\left(\frac{u}{p}\right) = \left(\frac{2^r}{p}\right)$, relation que l'on changera ensuite, comme à l'endroit cité, en celle-ci: $\left(\frac{u}{p}\right) = (-1)^{\frac{p-1}{4}}$.

Décomposons actuellement le nombre impair t en ses facteurs simples, en posant $t = gg'g'' \dots \times hh'h'' \dots$, où les nombres premiers $g, g', g'', \text{ etc.}$, $h, h', h'', \text{ etc.}$ sont tels que:

$$(\epsilon) \quad \begin{cases} \left(\frac{-a}{g}\right) = 1, & \left(\frac{-a}{g'}\right) = 1, & \left(\frac{-a}{g''}\right) = 1, \text{ etc.} \\ \left(\frac{-a}{h}\right) = -1, & \left(\frac{-a}{h'}\right) = -1, & \left(\frac{-a}{h''}\right) = -1, \text{ etc.} \end{cases}$$

L'équation $t^2-au^2 = p$ donne immédiatement:

$$\begin{cases} \left(\frac{-ap}{g}\right) = 1, & \left(\frac{-ap}{g'}\right) = 1, & \left(\frac{-ap}{g''}\right) = 1, \text{ etc.} \\ \left(\frac{-ap}{h}\right) = 1, & \left(\frac{-ap}{h'}\right) = 1, & \left(\frac{-ap}{h''}\right) = 1, \text{ etc.} \end{cases}$$

Comparant ces relations aux précédentes il viendra:

$$\begin{cases} \left(\frac{p}{g}\right) = 1, & \left(\frac{p}{g'}\right) = 1, & \left(\frac{p}{g''}\right) = 1, \text{ etc.} \\ \left(\frac{p}{h}\right) = -1, & \left(\frac{p}{h'}\right) = -1, & \left(\frac{p}{h''}\right) = -1, \text{ etc.} \end{cases}$$

L'application de la loi de réciprocité donnera ensuite, p étant de la forme $4n+1$:

$$\begin{cases} \left(\frac{g}{p}\right) = 1, & \left(\frac{g'}{p}\right) = 1, & \left(\frac{g''}{p}\right) = 1, \text{ etc.} \\ \left(\frac{h}{p}\right) = -1, & \left(\frac{h'}{p}\right) = -1, & \left(\frac{h''}{p}\right) = -1, \text{ etc.} \end{cases}$$

d'où l'on conclut en multipliant:

$$\left(\frac{gg'g'' \dots \times hh'h'' \dots}{p}\right) = \left(\frac{t}{p}\right) = \pm 1,$$

le signe supérieur ou inférieur ayant lieu selon que les nombres premiers h ,

h', h'', \dots sont en nombre pair ou impair. On peut énoncer ce résultat d'une manière un peu différente, en disant que $\left(\frac{t}{p}\right)$ est égal au produit des seconds membres des relations (ε).

On peut, dans les relations (ε), changer partout $-a$ en a , pourvu qu'en même temps on change le signe des seconds membres de celles de ces relations où il se trouve un nombre premier $g, g', g'', \dots, h, h', h'', \dots$ de la forme $4n+3$. On aura ainsi:

$$(\zeta) \quad \left\{ \begin{array}{l} \left(\frac{a}{g}\right) = \pm 1, \quad \left(\frac{a}{g'}\right) = \pm 1, \quad \left(\frac{a}{g''}\right) = \pm 1, \quad \text{etc.} \\ \left(\frac{a}{h}\right) = \pm 1, \quad \left(\frac{a}{h'}\right) = \pm 1, \quad \left(\frac{a}{h''}\right) = \pm 1, \quad \text{etc.} \end{array} \right.$$

En comparant le second membre de chacune de ces relations avec le second membre de la relation correspondante du tableau (ε), on trouvera autant de changements de signe qu'il y a de nombres premiers $4n+3$ parmi les nombres $g, g', g'', \dots, h, h', h'', \dots$.

Le nombre des changements sera donc pair, lorsque parmi les nombres $g, g', g'', \dots, h, h', h'', \dots$ il s'en trouve un nombre pair de la forme $4n+3$. Dans ce cas qui aura lieu toutes les fois que $t = gg'g'' \dots \times hh'h'' \dots$ est de la forme $4n+1$, le produit des seconds membres des relations (ζ) sera donc le même que le produit des seconds membres des relations (ε).

D'un autre côté, on peut, en vertu de la loi de réciprocité, renverser les premiers membres des relations (ζ), sans qu'il soit nécessaire de changer le signe d'aucun des seconds membres de ces relations. Le produit de toutes les expressions renversées, c'est-à-dire $\left(\frac{gg'g'' \dots \times hh'h'' \dots}{a}\right)$ ou $\left(\frac{t}{a}\right)$, est donc égal au produit des seconds membres des relations (ζ) et par conséquent aussi, d'après ce qu'on a vu précédemment, égal au produit des seconds membres des relations (ε). Or, ayant prouvé plus haut que ce dernier produit est égal à $\left(\frac{t}{p}\right)$, on a:

$$\left(\frac{t}{p}\right) = \left(\frac{t}{a}\right).$$

Ce résultat est relatif au cas où t est de la forme $4n+1$; si l'on examine d'une manière semblable le cas de $t = 4n+3$, on trouvera qu'on a alors:

$$\left(\frac{t}{p}\right) = -\left(\frac{t}{a}\right).$$

Ces deux cas sont compris dans la formule suivante à laquelle nous réunissons un résultat obtenu plus haut :

$$(i) \quad \left(\frac{t}{p}\right) = (-1)^{\frac{t-1}{2}} \left(\frac{t}{a}\right), \quad \left(\frac{u}{p}\right) = (-1)^{\frac{p-1}{4}}.$$

L'équation $t^2 - au^2 = p$ donne successivement :

$$t^2 \equiv au^2, \quad t^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{4}} u^{\frac{p-1}{2}} \pmod{p}.$$

d'où l'on voit que a sera ou ne sera pas résidu biquadratique relativement à p , selon que l'on a $\left(\frac{t}{p}\right) = \left(\frac{u}{p}\right)$ ou $\left(\frac{t}{p}\right) = -\left(\frac{u}{p}\right)$. En mettant à la place de $\left(\frac{t}{p}\right)$ et $\left(\frac{u}{p}\right)$ les valeurs données par les expressions (i), on pourra remplacer les conditions précédentes par celles qui suivent :

a sera ou ne sera pas résidu biquadratique par rapport à p , selon que l'on a :

$$(ii) \quad \left(\frac{t}{a}\right) = (-1)^{\frac{t-1}{2} + \frac{p-1}{4}} \quad \text{ou} \quad \left(\frac{t}{a}\right) = -(-1)^{\frac{t-1}{2} + \frac{p-1}{4}}.$$

résultat que nous ne nous arrêterons pas à démontrer.

Posons maintenant $p = g^2 + \psi^2$ (où ψ est supposé pair) et égalons cette valeur de p à celle que nous avons considérée précédemment. Nous aurons ainsi $p = t^2 - au^2 = g^2 + \psi^2$ d'où l'on conclut en transposant :

$$t^2 - \psi^2 = (t + \psi)(t - \psi) = g^2 + au^2.$$

Il y a maintenant deux cas à distinguer, selon que g est ou n'est pas divisible par a . Commençons par celui où g n'est pas divisible par a . Soit m le plus grand commun diviseur de g et de u , qui sera nécessairement impair et non divisible par a , et faisons $g = mg'$, $u = mu'$, valeurs dont la substitution dans l'équation obtenue plus haut la change en celle-ci :

$$(t + \psi)(t - \psi) = m^2(g'^2 + au'^2).$$

Cette équation fait voir que $t + \psi$ est composé de deux facteurs dont l'un divise m^2 , l'autre $g'^2 + au'^2$, et qu'il en est de même de $t - \psi$. Si nous désignons les facteurs de $t + \psi$ par E et K et ceux de $t - \psi$ par F et L , nous aurons :

$$\begin{aligned} t + \psi &= EK, & t - \psi &= FL, \\ m^2 &= EF, & g'^2 + au'^2 &= KL. \end{aligned}$$

On s'assurera, comme dans le paragraphe 4, que les nombres E et F sont premiers entre eux. Il suit de là et de l'équation $m^2 = EF$ que chacun de ces nombres est un carré, de sorte que :

$$\left(\frac{E}{a}\right) = 1, \quad \left(\frac{F}{a}\right) = 1.$$

La différence des nombres impairs $t+\psi$ et $t-\psi$ étant 2ψ et par conséquent divisible par 4, on voit que ces deux nombres sont ou l'un et l'autre de la forme $4n+1$, ou l'un et l'autre de la forme $4n+3$. Comme, d'un autre côté, les nombres E et F sont l'un et l'autre de la forme $4n+1$ (ces nombres étant des carrés impairs), il suit des équations $t+\psi = EK$, $t-\psi = FL$, que les nombres K et L sont ou l'un et l'autre de la forme $4n+1$ ou l'un et l'autre de la forme $4n+3$ et que le premier ou le second de ces cas a lieu, selon que les nombres $t+\psi$ et $t-\psi$ sont l'un et l'autre de la forme $4n+1$, ou l'un et l'autre de la forme $4n+3$. Distinguons maintenant deux cas, selon que p est de la forme $8n+1$ ou de celle-ci: $8n+5$. On voit, par l'équation $p^2 = g^2 + \psi^2$, que, dans le premier cas, ψ est divisible par 4, d'où il suit que $t+\psi$ et $t-\psi$ sont alors l'un et l'autre de la forme $4n+1$ ou l'un et l'autre de la forme $4n+3$, selon que t est de la forme $4n+1$, ou de celle-ci: $4n+3$. Le contraire a lieu dans le cas de $p = 8n+5$ et les résultats relatifs à ces deux cas peuvent être compris dans cet énoncé:

Les nombres $t+\psi$ et $t-\psi$, et par conséquent aussi les nombres K et L , sont l'un et l'autre de la forme $4n+1$ ou de celle-ci: $4n+3$, selon que $(-1)^{\frac{p-1}{4} + \frac{t-1}{2}}$ est égal à 1 ou à -1 .

Il résulte de l'équation $g'^2 + au'^2 = KL$ que les nombres K et L sont diviseurs de la formule $g'^2 + au'^2$ (où g' et au' sont premiers entre eux et où a désigne un nombre premier $4n+1$). Or, on sait que, si R désigne un diviseur impair d'une telle formule, on a:

$$\left(\frac{R}{a}\right) = 1, \quad \text{ou} \quad \left(\frac{R}{a}\right) = -1,$$

selon que R est de la forme $4n+1$ ou de la forme $4n+3$. (*Théorie des Nombres*, no. 196.)

Appliquant ce théorème aux nombres K et L , il viendra:

$$\left(\frac{K}{a}\right) = \left(\frac{L}{a}\right) = (-1)^{\frac{p-1}{4} + \frac{t-1}{2}},$$

d'où l'on conclura ensuite, en multipliant par les expressions $\left(\frac{E}{a}\right) = 1$, $\left(\frac{F}{a}\right) = 1$, trouvées plus haut:

$$\left(\frac{t+\psi}{a}\right) = \left(\frac{t-\psi}{a}\right) = (-1)^{\frac{p-1}{4} + \frac{t-1}{2}},$$

ou, ce qui revient au même, a étant un nombre premier $4n+1$:

$$\left(\frac{\psi+t}{a}\right) = \left(\frac{\psi-t}{a}\right) = (-1)^{\frac{p-1}{4} + \frac{t-1}{2}}.$$

Si l'on compare ce qui vient d'être prouvé au résultat (θ), obtenu plus haut, on verra que a est ou n'est pas résidu biquadratique relativement à p , selon que l'on a :

$$\left(\frac{\psi+t}{a}\right) = \left(\frac{\psi-t}{a}\right) = \left(\frac{t}{a}\right).$$

ou :

$$\left(\frac{\psi+t}{a}\right) = \left(\frac{\psi-t}{a}\right) = -\left(\frac{t}{a}\right).$$

L'équation $p = t^2 - at^2$ fait voir que, si l'on désigne par χ l'une quelconque des deux racines de la congruence $\chi^2 \equiv p \pmod{a}$, on a $t \equiv \chi$ ou $t \equiv -\chi \pmod{a}$. Il suit de là, a étant de la forme $4n+1$, $\left(\frac{t}{a}\right) = \left(\frac{\chi}{a}\right)$. D'un autre côté, comme en vertu de ce qui précède $\left(\frac{\psi+t}{a}\right) = \left(\frac{\psi-t}{a}\right)$, on voit qu'on a toujours :

$$\left(\frac{\psi+\chi}{a}\right) = \left(\frac{\psi+t}{a}\right) = \left(\frac{\psi-t}{a}\right).$$

On conclut de là, en ayant égard à ce qui a été dit il n'y a qu'un instant, que le nombre a sera résidu biquadratique par rapport à p , lorsqu'on a $\left(\frac{\chi+\psi}{a}\right) = \left(\frac{\chi}{a}\right)$ ou, ce qui est la même chose, lorsque $\left(\frac{\chi(\chi+\psi)}{a}\right) = 1$, et que a sera non-résidu biquadratique relativement à p , lorsqu'on a $\left(\frac{\chi+\psi}{a}\right) = -\left(\frac{\chi}{a}\right)$, ou, ce qui revient au même, lorsque $\left(\frac{\chi(\chi+\psi)}{a}\right) = -1$.

Ce résultat est relatif au cas où g n'est pas divisible par a . Reste à examiner le cas de g divisible par a . En traitant ce cas d'une manière semblable, on trouve que, lorsqu'il a lieu, l'un des nombres $t+\psi$, $t-\psi$ (nous le désignerons par $t\pm\psi$) est divisible par a et que, comme dans le premier cas, l'autre $t\mp\psi$ est tel que :

$$\left(\frac{t\mp\psi}{a}\right) = (-1)^{\frac{p-1}{4} + \frac{t-1}{2}},$$

ou, ce qui revient au même, en ajoutant à $t\mp\psi$ le nombre $t\pm\psi$, multiple de a :

$$\left(\frac{2t}{a}\right) = (-1)^{\frac{p-1}{4} + \frac{t-1}{2}}.$$

En comparant ceci à ce qui a été prouvé plus haut (θ), on trouvera que, dans le cas de g divisible par a , a est ou n'est pas résidu biquadratique relativement à p , selon que l'on a $\left(\frac{2}{a}\right) = 1$, ou $\left(\frac{2}{a}\right) = -1$, ou, ce qui est la

même chose, d'après un théorème connu, selon que a est de la forme $8n+1$ ou de la forme $8n+5$.

Il en est des résultats que nous venons d'obtenir comme de ceux que nous avons établis dans le paragraphe 4; ils ont encore lieu quand même p ne pourrait être mis sous la forme $t^2 - at^2$, et supposent uniquement que les nombres premiers $a = 4n+1$, et $p = 4n+1$, soient tels que $\left(\frac{a}{p}\right) = 1$. Pour les démontrer dans cette extension, il suffira de suivre la marche qui a été indiquée vers la fin du paragraphe 4, et de s'appuyer sur la proposition auxiliaire, dont il y est question et à l'énoncé de laquelle on a donné la généralité nécessaire pour qu'elle puisse servir de base, en même temps, à la démonstration du théorème général à la fin du paragraphe 4 et à celle du théorème que nous allons énoncer. Ces deux théorèmes n'en forment proprement qu'un, et en procédant, comme on l'a dit à l'endroit cité, c'est-à-dire en appliquant à l'équation $t^2 \pm Mt^2 = p$, où M désigne le produit d'un nombre quelconque de nombres premiers différents, des considérations analogues à celles qu'on a employées dans ce paragraphe et dans les précédents, on démontrera simultanément ces deux théorèmes, ou plutôt on arrivera à un théorème dans l'énoncé duquel ils se trouvent réunis.

Théorème II.

a désignant un nombre premier $4n+1$, et p un autre nombre premier $4n+1$, tel que $\left(\frac{a}{p}\right) = 1$, si l'on fait $p = g^2 + \psi^2$ (où ψ est supposé pair), on pourra décider de la manière suivante, si a est ou n'est pas résidu biquadratique par rapport à p . Si g est divisible par a , a sera ou ne sera pas résidu biquadratique relativement à p , selon que a est de la forme $8n+1$ ou de celle-ci: $8n+5$. Si g n'est pas divisible par a , on cherchera un nombre x tel qu'on ait $x^2 \equiv p \pmod{a}$. Cela posé, a sera ou ne sera pas résidu biquadratique par rapport à p , selon que l'on a $\left(\frac{x(x+\psi)}{a}\right) = 1$ ou $\left(\frac{x(x+\psi)}{a}\right) = -1$.

En faisant successivement $a = 5$, $a = 13$, on aura les théorèmes particuliers suivants qu'on doit regarder comme rigoureusement prouvés par ce qui précède, la formule $t^2 - at^2$ n'ayant, pour ces valeurs de a , d'autre diviseur quadratique que celui-ci: $t^2 - at^2$, ou en d'autres termes, tout diviseur de $t^2 - at^2$ étant lui-même de la forme $t^2 - at^2$.

p désignant un nombre premier de l'une des formes $20n+1$, $20n+9$, si l'on fait $p = \varphi^2 + \psi^2$ (où ψ est supposé pair) on s'assure facilement que l'un des nombres φ , ψ est multiple de 5. Cela posé, je dis que 5 sera ou ne sera pas résidu biquadratique relativement à p , selon que c'est ψ ou φ qui est divisible par 5.⁴

etc.

En indiquant plus haut une méthode qui pourrait servir à établir dans toute leur généralité les théorèmes I et II, nous avons dit qu'en suivant cette méthode on se trouvait dans la nécessité de s'appuyer sur une proposition subsidiaire qu'il paraît assez difficile de démontrer en toute rigueur. En réfléchissant à cet inconvénient, j'ai reconnu qu'il était très facile d'y remédier en modifiant un peu la marche tracée plus haut. Cette modification est extrêmement légère et consiste en ce qu'au lieu de considérer les équations $t^2 - bu^2 = p$, $t^2 - au^2 = p$, qui peuvent n'être pas possibles quoiqu'on ait $\left(\frac{b}{p}\right) = 1$, $\left(\frac{a}{p}\right) = 1$, il faut appliquer des considérations du genre des précédentes aux équations plus générales $t^2 - bu^2 = ps^2$, $t^2 - au^2 = ps^2$ (on remplace avec avantage la dernière par celle-ci: $t^2 + au^2 = ps$, qui peut être traitée plus simplement), auxquelles on peut toujours satisfaire, lorsque les conditions $\left(\frac{b}{p}\right) = 1$, $\left(\frac{a}{p}\right) = 1$ ont lieu, comme il résulte du beau théorème que M. LEGENDRE a donné pour juger de la possibilité ou de l'impossibilité de l'équation $\alpha x^2 + \beta y^2 = \gamma z^2$ (*Théorie des Nombres*, no. 27).

La démonstration ainsi modifiée, outre qu'elle est entièrement rigoureuse, a encore l'avantage d'une plus grande simplicité, comme tout lecteur qui a bien saisi l'esprit des considérations précédentes pourra en juger, en développant cette démonstration d'après l'indication qu'on vient d'en donner.

Addition au mémoire précédent.

Quoique l'indication que nous avons donnée à la fin du mémoire précédent sur la marche à suivre pour établir d'une manière entièrement rigoureuse les théorèmes I et II de notre mémoire, puisse suffire à tout lecteur familiarisé avec l'analyse indéterminée, nous croyons ne pas faire une chose inutile, en développant avec détail, dans cette addition, les démonstrations des théorèmes dont il s'agit, ces démonstrations étant susceptibles d'être beaucoup

simplifiées au moyen de quelques considérations qui peuvent ne pas se présenter de suite à l'esprit. Nous commençons par la démonstration du premier des théorèmes cités.

Désignons par p un nombre premier $4n+1$, par b un nombre premier $4n+3$, tel que $\left(\frac{b}{p}\right) = 1$, et considérons l'équation:

$$(a') \quad t^2 - bu^2 = ps^2.$$

D'après le théorème déjà cité (*Théorie des Nombres*, no. 27), les conditions nécessaires pour que cette équation soit possible sont celles-ci: $\left(\frac{b}{p}\right) = 1$ et $\left(\frac{p}{b}\right) = 1$. Or, de ces conditions la première a lieu par hypothèse et quant à la seconde, il suit du théorème connu sous le nom de loi de réciprocité, qu'elle a toujours lieu lorsque la première est satisfaite. L'équation est donc résoluble. Il est évident qu'on peut supposer que les nombres t , u , s , qui y satisfont, sont premiers entre eux, comparés deux à deux. L'équation étant dans cet état, ces trois nombres seront l'un pair, les deux autres impairs, et on s'assure facilement que s ne saurait être pair. Le nombre s étant impair, les nombres t , u seront l'un pair, l'autre impair et il y aurait deux cas à examiner selon que t est pair ou impair. Mais quoique ces deux cas soient susceptibles d'être traités par la même analyse, il est plus simple de n'en considérer qu'un seul, celui de t impair par exemple, et de montrer que l'autre peut y être facilement ramené. Faisons donc voir qu'il est toujours permis de supposer t impair dans l'équation $t^2 - bu^2 = ps^2$. Si t était pair dans l'équation (a'), on déduirait des nombres t , u , par le moyen indiqué dans la note relative au commencement du paragraphe 3 du mémoire précédent, d'autres nombres t' (impair), u' (pair) tels que $t'^2 - bu'^2 = ps^2$. Nous pourrions donc considérer t comme impair dans tout ce qui va suivre.

Décomposons les nombres t et u en leurs facteurs simples, en faisant:

$$t = UV' \dots, \quad u = 2^r k k' k'' \dots,$$

l, l', l'', \dots et k, k', k'', \dots désignant des nombres premiers impairs. La seule inspection de l'équation (a') donne:

$$\left(\frac{p}{k}\right) = 1, \quad \left(\frac{p}{k'}\right) = 1, \quad \left(\frac{p}{k''}\right) = 1, \quad \dots$$

On aura ensuite, en appliquant la loi de réciprocité, p étant un nombre premier $4n+1$:

$$\left(\frac{k}{p}\right) = 1, \quad \left(\frac{k'}{p}\right) = 1, \quad \left(\frac{k''}{p}\right) = 1, \quad \dots$$

Faisant le produit de toutes ces expressions et de la formule identique $\left(\frac{2^v}{p}\right) = \left(\frac{2^v}{p}\right)$, il viendra :

$$\left(\frac{2^v k k' k'' \dots}{p}\right) = \left(\frac{u}{p}\right) = \left(\frac{2^v}{p}\right).$$

Le nombre p est de l'une des deux formes $8n+1$, $8n+5$. Si p est de la première forme, on a, en vertu d'un théorème connu, $\left(\frac{2}{p}\right) = 1$, et par conséquent aussi $\left(\frac{2^v}{p}\right) = 1$. Donc $\left(\frac{u}{p}\right) = 1$. Si p est de la forme $8n+5$, le nombre u sera impairement pair, de sorte que $v = 1$, et comme on a, d'un autre côté, pour les nombres premiers $p = 8n+5$, $\left(\frac{2}{p}\right) = -1$, il viendra $\left(\frac{u}{p}\right) = -1$. Les deux cas dont il vient d'être question sont compris dans la formule :

$$(\beta') \quad \left(\frac{u}{p}\right) = (-1)^{\frac{p-1}{4}}.$$

Reprenons l'équation (α') de laquelle nous tirons immédiatement :

$$\left(\frac{-b}{l}\right) = \left(\frac{p}{l}\right), \quad \left(\frac{-b}{l'}\right) = \left(\frac{p}{l'}\right), \quad \left(\frac{-b}{l''}\right) = \left(\frac{p}{l''}\right), \quad \dots$$

Comme p est un nombre premier $4n+1$, et b un nombre premier $4n+3$, on trouvera en appliquant la loi de réciprocité :

$$\left(\frac{l}{b}\right) = \left(\frac{l}{p}\right), \quad \left(\frac{l'}{b}\right) = \left(\frac{l'}{p}\right), \quad \left(\frac{l''}{b}\right) = \left(\frac{l''}{p}\right), \quad \dots$$

La multiplication donnera ensuite :

$$\left(\frac{ll'l'' \dots}{b}\right) = \left(\frac{ll'l'' \dots}{p}\right).$$

ou, ce qui revient au même :

$$(\gamma') \quad \left(\frac{t}{b}\right) = \left(\frac{t}{p}\right).$$

En mettant l'équation (α') sous la forme d'une congruence, on aura :

$$t^2 \equiv bu^2 \pmod{p}.$$

On conclut de là, en élevant les deux membres à la puissance $\frac{p-1}{4}$:

$$t^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{4}} u^{\frac{p-1}{2}} \pmod{p},$$

ou, ce qui revient au même, en remplaçant $u^{\frac{p-1}{2}}$ par sa valeur $(-1)^{\frac{p-1}{4}}$ donnée par la formule (β') :

$$t^{\frac{p-1}{2}} \equiv (-b)^{\frac{p-1}{4}} \pmod{p}.$$

Cette dernière congruence fait voir que $-b$ est ou n'est pas résidu biquadratique relativement à p , selon que l'on a $\left(\frac{t}{p}\right) = 1$, ou $\left(\frac{t}{p}\right) = -1$. Si l'on compare ce résultat à la formule (γ'), on obtiendra cet énoncé:

$$(\delta') \quad -b \text{ est ou n'est pas résidu biquadratique par rapport à } p, \text{ selon} \\ \text{que l'on a } \left(\frac{t}{b}\right) = 1 \text{ ou } \left(\frac{t}{b}\right) = -1.$$

Décomposons actuellement le nombre premier p en deux carrés, en posant $p = g^2 + \psi^2$ (où ψ est supposé pair) et mettons cette valeur de p dans l'équation (α'). Il viendra ainsi:

$$t^2 - bu^2 = s^2g^2 + s^2\psi^2,$$

et l'on aura ensuite en transposant:

$$t^2 - \psi^2s^2 = (t + \psi s)(t - \psi s) = s^2g^2 + bu^2.$$

Les nombres s, t, u étant deux à deux premiers entre eux, on voit par l'équation (α') que s ne saurait être divisible par b . Nous distinguerons maintenant deux cas selon que g est ou n'est pas divisible par b , et nous examinerons d'abord le dernier de ces deux cas. Si nous désignons par m le plus grand diviseur commun de g et u , m sera impair et non-divisible par b comme g . Posons $g = mg'$, $u = mu'$ et substituons ces valeurs dans la dernière équation. Il viendra ainsi:

$$(t + \psi s)(t - \psi s) = m^2(s^2g'^2 + bu'^2).$$

Comme sg' et bu' sont premiers entre eux, d'après ce qui précède, il suit d'un théorème connu, conséquence très simple de la loi de réciprocité (*Théorie des Nombres* no. 197), que tout diviseur R du facteur binôme du second membre qui est évidemment impair, est tel que $\left(\frac{R}{b}\right) = 1$.

La dernière équation fait voir que chacun des nombres $t + \psi s$, $t - \psi s$ est composé de deux facteurs, l'un diviseur de m^2 , l'autre diviseur de $s^2g'^2 + bu'^2$. Si nous désignons ces 4 facteurs par E, F, K et L , nous aurons les équations:

$$t + \psi s = EK, \quad m^2 = EF, \\ t - \psi s = FL, \quad g'^2s^2 + bu'^2 = KL.$$

Il est facile de s'assurer que les nombres E et F , qui sont impairs l'un et l'autre, comme diviseurs de m^2 , sont premiers entre eux. En effet, si ces nombres étaient divisibles l'un et l'autre par un même nombre premier δ , δ diviserait chacun des nombres $t + \psi s$, $t - \psi s$ et par conséquent aussi leur demi-somme et leur demi-différence, c'est-à-dire les nombres t et ψs . D'un autre

côté, comme δ divise m^2 , il divisera aussi le nombre g , g étant égal à mg' ; il suit de là et de ce que $g^2 + \psi^2$ est égal au nombre premier p , que ψ n'est pas divisible par b . Il faudrait donc, d'après ce qui précède, que δ fût diviseur commun de t et s , ce qui est impossible, ces nombres étant premiers entre eux. Donc les nombres E et F sont premiers entre eux, et comme leur produit est un carré, chacun d'eux sera pareillement un carré. On a donc:

$$\left(\frac{E}{b}\right) = 1, \quad \left(\frac{F}{b}\right) = 1.$$

On a aussi:

$$\left(\frac{K}{b}\right) = 1, \quad \left(\frac{L}{b}\right) = 1.$$

K et L étant des diviseurs de $s^2g'^2 + bu^2$. On conclut de là, en multipliant:

$$\left(\frac{EK}{b}\right) = 1, \quad \left(\frac{FL}{b}\right) = 1,$$

ou, ce qui est la même chose:

$$\left(\frac{t+\psi s}{b}\right) = 1, \quad \left(\frac{t-\psi s}{b}\right) = 1.$$

Si l'on fait attention que b est un nombre premier $4n+3$, on pourra présenter de cette autre manière la dernière de ces relations:

$$\left(\frac{\psi s - t}{b}\right) = -1.$$

Cela étant, on voit qu'on peut les comprendre l'une et l'autre dans cette formule:

$$(\varepsilon') \quad \left(\frac{\psi s \pm t}{b}\right) = \pm 1,$$

où les signes sont à volonté, mais les mêmes dans les deux membres.

Comme on a $\left(\frac{p}{b}\right) = 1$, la congruence $\chi^2 \equiv p \pmod{b}$ est possible et a, comme l'on sait, deux racines entre les limites $-\frac{1}{2}b$ et $\frac{1}{2}b$. Désignons par χ l'une de ces racines prise au hasard. L'équation (α') donne cette congruence: $t^2 \equiv ps^2 \pmod{b}$. Si l'on compare celle-ci à la précédente, on aura $t^2 \equiv \chi^2 s^2 \pmod{b}$. On conclut de là $\pm t \equiv \chi s \pmod{b}$, le signe étant tantôt positif, tantôt négatif et dépendant du choix que l'on aura fait entre les deux racines de la congruence $\chi^2 \equiv p \pmod{b}$. Les signes étant à volonté dans la formule (ε'), on peut supposer qu'ils y sont les mêmes que dans celle-ci: $\pm t \equiv \chi s \pmod{b}$. Remplaçant $\pm t$ par le nombre χs qui ne diffère de $\pm t$ que par un multiple de b , il viendra:

$$\left(\frac{\psi s + \chi s}{b}\right) = \pm 1.$$

D'un autre côté, si l'on se rappelle que b est de la forme $4n+3$, on tirera de la formule $\pm t \equiv \chi s \pmod{b}$: $\pm \left(\frac{t}{b}\right) = \left(\frac{\chi s}{b}\right)$. Si l'on multiplie cette égalité par la précédente, on aura, les signes étant les mêmes dans ces deux formules:

$$\left(\frac{\chi(\chi+\psi)}{b}\right)\left(\frac{s^2}{b}\right) = \left(\frac{t}{b}\right)$$

ou, ce qui revient au même:

$$\left(\frac{\chi(\chi+\psi)}{b}\right) = \left(\frac{t}{b}\right).$$

Si l'on compare cette formule avec ce qui a été prouvé plus haut (d'), on obtiendra ce résultat:

$$(\xi') \quad \begin{array}{l} -b \text{ est ou n'est pas résidu biquadratique par rapport à } p, \\ \text{selon que l'on a } \left(\frac{\chi(\chi+\psi)}{b}\right) = 1 \text{ ou } \left(\frac{\chi(\chi+\psi)}{b}\right) = -1. \end{array}$$

Cette proposition est relative au cas où g n'est pas divisible par b . Examinons maintenant le cas de g divisible par b . Soient b^{l+k} et b^h respectivement les puissances les plus élevées de b qui divisent g et u (k et h pouvant être nuls), soit de plus m le plus grand commun diviseur de $\frac{g}{b^{l+k}}$ et $\frac{u}{b^h}$. Si nous faisons $g = b^{l+k}m g'$, $u = b^h m u'$, les nombres g' et u' , dont le premier est impair, le second pair, seront premiers entre eux, et non-divisibles par b , et m sera impair et non-divisible par b . La substitution des valeurs précédentes donne cette équation:

$$(t+\psi s)(t-\psi s) = m^2 [b^{2k+2}(s g')^2 + b^{2h+1}u'^2].$$

Il faut maintenant distinguer deux cas selon que l'on a $k \geq h$ ou $k < h$. Dans le premier, le facteur binôme du second membre peut être mis sous cette forme:

$$b^{2h+1}[u'^2 + b(b^{k-h} s g')^2],$$

où il faut remarquer que les nombres u' et $b^{k-h} s g'$ sont premiers entre eux. Dans le cas de $k < h$, on mettra le facteur binôme sous la forme suivante:

$$b^{2k+2}[(s g')^2 + b(b^{h-k-1} u')^2],$$

où les nombres $s g'$ et $b^{h-k-1} u'$ sont premiers entre eux. On voit donc que le facteur binôme est toujours le produit d'une puissance de b et d'une expression impaire telle que $g^2 + b h^2$, dans laquelle g et $b h$ sont premiers entre eux. Désignant par b^r la puissance de b dont il s'agit, on pourra donc écrire la der-

nière équation de cette manière :

$$(t+\psi s)(t-\psi s) = m^2 b'(g^2+bh^2).$$

Les nombres $t+\psi s$, $t-\psi s$ ne sauraient être divisibles l'un et l'autre par b , puisqu'alors leur demi-somme qui est t , le serait aussi, ce qu'on a vu plus haut être impossible. Si l'on désigne par $t\pm\psi s$ celui de ces deux nombres qui est divisible par b , on aura $t\pm\psi s \equiv 0 \pmod{b}$ et je dis que l'autre $t\mp\psi s$ est tel que $\left(\frac{t\mp\psi s}{b}\right) = 1$. En effet $t\mp\psi s$ est composé de deux facteurs E et K dont le premier E divise m^2 , le second g^2+bh^2 .

Or, on s'assure, comme dans le cas de g non-divisible par b , que E est un carré, de sorte qu'on a $\left(\frac{E}{b}\right) = 1$. On a aussi $\left(\frac{K}{b}\right) = 1$, K étant diviseur de g^2+bh^2 . On conclut de là en multipliant :

$$\left(\frac{EK}{b}\right) = \left(\frac{t\mp\psi s}{b}\right) = 1.$$

Il est permis d'augmenter $t\mp\psi s$ dans cette formule d'un multiple quelconque de b . Ajoutant le nombre $t\pm\psi s$ qu'on a vu être un tel multiple, il viendra $\left(\frac{2t}{b}\right) = 1$ ou, ce qui revient au même: $\left(\frac{t}{b}\right) = \left(\frac{2}{b}\right)$, résultat dont la comparaison avec un théorème connu fait voir que dans le cas de g divisible par b , on a $\left(\frac{t}{b}\right) = 1$ ou $\left(\frac{t}{b}\right) = -1$, selon que b est de la forme $8n+7$ ou de celle-ci: $8n+3$. Si l'on combine ceci avec le résultat obtenu plus haut (d'), on trouve que, lorsque g est multiple de b :

$-b$ est ou n'est pas résidu biquadratique par rapport à p , selon que b est de la forme $8n+7$ ou de celle-ci: $8n+3$.

En réunissant ce dernier résultat à celui auquel nous sommes parvenu plus haut (d'), on aura le théorème I énoncé à la fin du paragraphe 4 du mémoire précédent, théorème qui se trouve ainsi établi d'une manière très simple et entièrement rigoureuse.

Occupons-nous maintenant de la démonstration du théorème II. Désignons, comme dans tout ce qui précède, par a un nombre premier $4n+1$ et par p un autre nombre premier également de la forme $4n+1$ et tel que $\left(\frac{a}{p}\right) = 1$. On conclut de là, en appliquant la loi de réciprocité, qu'on a aussi $\left(\frac{p}{a}\right) = 1$. Ces conditions ayant lieu, il suit du théorème déjà cité plusieurs

fois, que l'équation:

$$(4') \quad t^2 + au^2 = ps^2,$$

peut être résolue. Si l'on suppose que les nombres t , u , s , comparés deux à deux, n'ont pas de diviseur commun, s sera impair et les deux autres seront l'un pair, l'autre impair, comme il est très facile de le voir. Il est évident en outre que, si l'équation est dans cet état, u n'est pas divisible par p , s ne l'est pas par a , et t n'est divisible ni par a ni par p .

Décomposons les nombres t et u en leurs facteurs simples, en faisant $u = 2^r k k' k'' \dots$, $t = 2^a l l' l'' \dots$, $k, k', k'' \dots$ et $l, l', l'' \dots$ désignant des nombres premiers impairs, et l'un des nombres μ, ν étant égal à zéro.

L'équation (4') donne d'abord:

$$\left(\frac{p}{k}\right) = 1, \quad \left(\frac{p}{k'}\right) = 1, \quad \left(\frac{p}{k''}\right) = 1, \quad \dots$$

d'où l'on conclut ensuite en appliquant la loi de réciprocité:

$$\left(\frac{k}{p}\right) = 1, \quad \left(\frac{k'}{p}\right) = 1, \quad \left(\frac{k''}{p}\right) = 1, \quad \dots$$

Faisant le produit des équations précédentes et de l'équation identique $\left(\frac{2^r}{p}\right) = \left(\frac{2^r}{p}\right)$, il viendra:

$$\left(\frac{2^r k k' k'' \dots}{p}\right) = \left(\frac{u}{p}\right) = \left(\frac{2^r}{p}\right).$$

Il résulte encore de l'équation (4'), qu'on a:

$$\left(\frac{a}{l}\right) = \left(\frac{p}{l}\right), \quad \left(\frac{a}{l'}\right) = \left(\frac{p}{l'}\right), \quad \left(\frac{a}{l''}\right) = \left(\frac{p}{l''}\right), \quad \dots$$

Comme les nombres premiers a et p sont l'un et l'autre de la forme $4n+1$, on conclut de là, en vertu de la loi de réciprocité:

$$\left(\frac{l}{a}\right) = \left(\frac{l}{p}\right), \quad \left(\frac{l'}{a}\right) = \left(\frac{l'}{p}\right), \quad \left(\frac{l''}{a}\right) = \left(\frac{l''}{p}\right), \quad \dots$$

Multipliant entre elles toutes ces relations, il viendra l'équation:

$$\left(\frac{l l' l'' \dots}{a}\right) = \left(\frac{l l' l'' \dots}{p}\right),$$

qui, si l'on multiplie ses deux membres par $\left(\frac{2^a}{a}\right)\left(\frac{2^a}{p}\right)$, se change en celle-ci:

$$\left(\frac{t}{a}\right)\left(\frac{2^a}{p}\right) = \left(\frac{t}{p}\right)\left(\frac{2^a}{a}\right).$$

Distinguons actuellement deux cas, selon que u est pair ou impair. Si

u est pair, t est impair; on a donc alors $\mu = 0$, et la dernière égalité se réduit à celle-ci:

$$\left(\frac{t}{a}\right) = \left(\frac{t}{p}\right).$$

Quant à la relation $\left(\frac{u}{p}\right) = \left(\frac{2^\nu}{p}\right)$, il est facile de voir qu'elle équivaut, dans ce cas, à celle-ci:

$$\left(\frac{u}{p}\right) = (-1)^{\frac{\nu-1}{4}}.$$

Pour s'en convaincre, il suffit de remarquer que, si p est de la forme $8n+1$, on a $\left(\frac{2}{p}\right) = 1$, et par conséquent aussi $\left(\frac{2^\nu}{p}\right) = 1$, et que, si p a la forme $8n+5$, ν est égal à l'unité et qu'on a pour tout nombre premier $p = 8n+5$, $\left(\frac{2}{p}\right) = -1$.

Passons à l'autre cas qui est celui de t pair et u impair. On a alors $\nu = 0$, ce qui réduit l'équation $\left(\frac{u}{p}\right) = \left(\frac{2^\nu}{p}\right)$ à $\left(\frac{u}{p}\right) = 1$.

Si les nombres p et a sont l'un et l'autre de la forme $8n+1$, ou l'un et l'autre de la forme $8n+5$, on a $\left(\frac{2}{a}\right) = \left(\frac{2}{p}\right)$ et par conséquent aussi $\left(\frac{2^a}{a}\right) = \left(\frac{2^a}{p}\right)$, et l'égalité $\left(\frac{t}{p}\right)\left(\frac{2^a}{a}\right) = \left(\frac{t}{a}\right)\left(\frac{2^a}{p}\right)$ se change en celle-ci: $\left(\frac{t}{p}\right) = \left(\frac{t}{a}\right)$. Si, au contraire, les nombres a, p sont l'un de la forme $8n+1$, l'autre de la forme $8n+5$, on a $\left(\frac{2}{a}\right) = -\left(\frac{2}{p}\right)$. D'un autre côté, l'équation $(4')$ fait voir que, dans ce cas, le nombre t est impairement pair, de sorte que $\mu = 1$. On a donc alors $\left(\frac{t}{p}\right) = -\left(\frac{t}{a}\right)$. Ces deux résultats sont compris dans la formule:

$$\left(\frac{t}{p}\right) = \left(\frac{t}{a}\right)(-1)^{\frac{a-1}{4} + \frac{p-1}{4}}.$$

Si nous réunissons tout ce que nous venons de prouver, nous aurons cet énoncé:

Si u est pair, on a $\left(\frac{t}{p}\right) = \left(\frac{t}{a}\right)$, $\left(\frac{u}{p}\right) = (-1)^{\frac{\nu-1}{4}}$; si u est impair,

on a $\left(\frac{t}{p}\right) = \left(\frac{t}{a}\right)(-1)^{\frac{p-1}{4} + \frac{a-1}{4}}$, $\left(\frac{u}{p}\right) = 1$.

En comparant ce résultat avec la congruence $t^{\frac{p-1}{2}} \equiv (-a)^{\frac{p-1}{4}} u^{\frac{p-1}{2}} \pmod{p}$, qui se déduit immédiatement de l'équation $(4')$, on trouvera ce théorème:

Si u est pair, a est ou n'est pas résidu biquadratique par rapport à p , selon que l'on a :

$$(g') \quad \left(\frac{t}{a}\right) = 1 \quad \text{ou} \quad \left(\frac{t}{a}\right) = -1;$$

si u est impair, a est ou n'est pas résidu biquadratique relativement à p , selon que l'on a :

$$\left(\frac{t}{a}\right) = (-1)^{\frac{a-1}{4}} \quad \text{ou} \quad \left(\frac{t}{a}\right) = -(-1)^{\frac{a-1}{4}}.$$

Décomposons p en deux carrés, en posant $p = g^2 + \psi^2$ (ψ étant supposé pair). La substitution de cette valeur dans l'équation (g') donnera :

$$(t + \psi s)(t - \psi s) = g^2 s^2 - au^2.$$

Nous distinguerons maintenant deux cas selon que g est ou n'est pas divisible par a .

Premier cas: g n'est pas divisible par a .

Comme g est impair et non-divisible par a , le plus grand commun diviseur de g et de u , que nous désignerons par m , sera aussi impair et non-divisible par a . Si nous faisons $g = mg'$, $u = mu'$, l'équation précédente se changera en celle-ci :

$$(t + \psi s)(t - \psi s) = m^2(g'^2 s^2 - au'^2);$$

s est premier à au et par conséquent aussi à au' , g' est également premier à au' ; donc $g's$ et au' n'ont pas de diviseur commun. Cela étant, il suit d'un théorème connu (*Théorie des Nombres* no. 197) que tout diviseur impair R de $s^2 g'^2 - au'^2$ est tel qu'on a $\left(\frac{R}{a}\right) = 1$.

Désignant par E , K , F et L quatre indéterminées, nous pourrions remplacer la dernière équation par celles que je vais écrire :

$$\begin{aligned} t + \psi s &= EK, & m^2 &= EF, \\ t - \psi s &= FL, & (sg')^2 - au'^2 &= KL. \end{aligned}$$

On s'assure facilement que les nombres impairs E et F sont premiers entre eux. Il suit de là que chacun d'eux est un carré, de sorte qu'on a :

$$\left(\frac{E}{a}\right) = 1, \quad \left(\frac{F}{a}\right) = 1.$$

Il faut maintenant considérer successivement le cas de u pair et celui de u impair. Si u est pair, $u' = \frac{u}{m}$ le sera pareillement, et comme sg' est toujours impair, $(sg')^2 - au'^2$ sera également impair. Les nombres K et L seront donc

dans ce cas impairs l'un et l'autre, et comme ils divisent le binôme précédent, on aura :

$$\left(\frac{K}{a}\right) = 1, \quad \left(\frac{L}{a}\right) = 1.$$

Multipliant ces relations par celles que nous venons d'écrire, il viendra :

$$\left(\frac{EK}{a}\right) = \left(\frac{t+\psi s}{a}\right) = 1, \quad \left(\frac{FL}{a}\right) = \left(\frac{t-\psi s}{a}\right) = 1.$$

Comme a est un nombre premier $4n+1$, il est permis d'écrire la formule $\left(\frac{t-\psi s}{a}\right) = 1$ de cette autre manière : $\left(\frac{\psi s-t}{a}\right) = 1$. On a donc, dans le cas de n pair, $\left(\frac{\psi s \pm t}{a}\right) = 1$, le double signe étant à volonté.

Passons au cas où n est impair. Le nombre $u' = \frac{u}{m}$ sera également impair dans ce cas, et comme les carrés impairs $(sg')^2$, u'^2 sont de la forme $8n+1$, on voit que le binôme $(sg')^2 - au'^2$ sera de la forme $8n$ ou de la forme $8n+4$, selon que a est de la forme $8n+1$ ou de celle-ci : $8n+5$. Il est facile de s'assurer que, si a est de la forme $8n+1$, on a $\left(\frac{K}{a}\right) = 1$, $\left(\frac{L}{a}\right) = 1$. En effet, si l'on fait $K = 2^j K'$, 2^j étant la puissance la plus élevée de 2 qui divise K , K' sera un diviseur impair de $(sg')^2 - au'^2$ et l'on aura $\left(\frac{K'}{a}\right) = 1$. D'un autre côté, on sait, par un théorème connu, que tout nombre premier $a = 8n+1$, est tel que $\left(\frac{2}{a}\right) = 1$. On conclut de là $\left(\frac{2^j}{a}\right) = 1$, et multipliant ensuite par $\left(\frac{K'}{a}\right) = 1$, il viendra $\left(\frac{K}{a}\right) = 1$. On prouve d'une manière toute semblable qu'on a aussi $\left(\frac{L}{a}\right) = 1$. Multipliant ces relations par les suivantes : $\left(\frac{E}{a}\right) = 1$, $\left(\frac{F}{a}\right) = 1$, obtenues plus haut, il viendra :

$$\left(\frac{EK}{a}\right) = \left(\frac{t+\psi s}{a}\right) = 1, \quad \left(\frac{FL}{a}\right) = \left(\frac{t-\psi s}{a}\right) = 1.$$

Il est facile de voir que ces résultats, qui ont lieu lorsque n est impair et qu'en même temps a est de la forme $8n+1$, peuvent être réunis dans la formule $\left(\frac{\psi s \pm t}{a}\right) = 1$, où le double signe est à volonté.

Le nombre n étant toujours impair, supposons a de la forme $8n+5$. Le produit KL , qui équivaut au binôme $(sg')^2 - au'^2$, étant alors de la forme $8n+4$, et les nombres K et L étant évidemment pairs l'un et l'autre, chacun

d'eux sera de la forme $4n+2$, de sorte qu'en faisant $K = 2K'$, $L = 2L'$, K' et L' seront impairs: et comme ces derniers nombres sont en outre diviseurs de $(sg')^2 - au^2$, il suit de ce qui a été dit plus haut, qu'on a $\left(\frac{K'}{a}\right) = 1$, $\left(\frac{L'}{a}\right) = 1$. Mais on a, d'un autre côté, a étant de la forme $8n+5$, $\left(\frac{2}{a}\right) = -1$. Multipliant par les égalités précédentes, il viendra d'abord $\left(\frac{K}{a}\right) = -1$, $\left(\frac{L}{a}\right) = -1$, et si l'on multiplie ensuite avec les égalités $\left(\frac{E}{a}\right) = 1$, $\left(\frac{F}{a}\right) = 1$, trouvées plus haut, on aura:

$$\left(\frac{EK}{a}\right) = \left(\frac{t+\psi s}{a}\right) = -1, \quad \left(\frac{FL}{a}\right) = \left(\frac{t-\psi s}{a}\right) = -1.$$

Ces résultats, qui sont relatifs au cas où u est impair et où le nombre a est de la forme $8n+5$, sont compris dans la double formule:

$$\left(\frac{\psi s \pm t}{a}\right) = -1.$$

En résumant tout ce qui précède, on aura cet énoncé:

„Si u est pair, on a $\left(\frac{\psi s \pm t}{a}\right) = 1$; si, au contraire, u est impair, on a $\left(\frac{\psi s \pm t}{a}\right) = (-1)^{\frac{a-1}{4}}$, le double signe étant à volonté dans l'un et l'autre cas.”

On a vu plus haut (\mathcal{G}') que, lorsque u est pair, a est ou n'est pas résidu biquadratique par rapport à p , selon que l'on a $\left(\frac{t}{a}\right) = 1$, ou $\left(\frac{t}{a}\right) = -1$. D'un autre côté, il résulte de ce qui précède, qu'on a, dans ce même cas, $\left(\frac{\psi s \pm t}{a}\right) = 1$. On conclut de là que, si u est pair, a est ou n'est pas résidu biquadratique relativement à p , selon que l'on a:

$$\left(\frac{t}{a}\right) = \left(\frac{\psi s \pm t}{a}\right) \quad \text{ou} \quad \left(\frac{t}{a}\right) = -\left(\frac{\psi s \pm t}{a}\right).$$

On a également vu plus haut (\mathcal{G}') que, lorsque u est impair, a est ou n'est pas résidu biquadratique par rapport à p , selon que l'on a:

$$\left(\frac{t}{a}\right) = (-1)^{\frac{a-1}{4}} \quad \text{ou} \quad \left(\frac{t}{a}\right) = -(-1)^{\frac{a-1}{4}}.$$

D'un autre côté, l'énoncé précédent fait voir, qu'on a, dans le cas de u impair, $\left(\frac{\psi s \pm t}{a}\right) = (-1)^{\frac{a-1}{4}}$. En comparant ces deux résultats, on conclut que, lorsque

u est impair, a est ou n'est pas résidu biquadratique relativement à p , selon que l'on a :

$$\left(\frac{t}{a}\right) = \left(\frac{\psi s \pm t}{a}\right) \quad \text{ou} \quad \left(\frac{t}{a}\right) = -\left(\frac{\psi s \pm t}{a}\right).$$

La conclusion étant la même dans le cas de u pair et dans celui de u impair, on peut énoncer ce théorème :

„Si a est résidu biquadratique relativement à p , on a $\left(\frac{t}{a}\right) = \left(\frac{\psi s \pm t}{a}\right)$; si, au contraire, a n'est pas résidu biquadratique par rapport à p , on a $\left(\frac{t}{a}\right) = -\left(\frac{\psi s \pm t}{a}\right)$, le double signe étant à volonté dans l'un et l'autre cas.”

Comme on a $\left(\frac{p}{a}\right) = 1$, la congruence $x^2 = p \pmod{a}$ sera possible et aura, comme on sait, deux racines entre les limites $-\frac{1}{2}a$ et $\frac{1}{2}a$. Supposons que x désigne indistinctement l'une ou l'autre de ces racines. On tire immédiatement de l'équation (u'): $t^2 \equiv ps^2 \pmod{a}$, congruence dont la comparaison avec la précédente donne $t^2 \equiv x^2 s^2$, $\pm t \equiv xs \pmod{a}$, le signe supérieur ayant lieu pour l'une et le signe inférieur pour l'autre des deux racines de la congruence $x^2 = p \pmod{a}$. Si a est résidu biquadratique relativement à p , on a, comme on l'a vu il n'y a qu'un instant, $\left(\frac{t}{a}\right) = \left(\frac{\psi s \pm t}{a}\right)$. Le double signe étant à volonté dans cette formule, nous pouvons le supposer égal à celui qui se trouve dans la congruence $\pm t \equiv xs \pmod{a}$. Si nous remplaçons $\pm t$ par xs , il viendra :

$$\left(\frac{t}{a}\right) = \left(\frac{\psi s + xs}{a}\right) = \left(\frac{\psi + x}{a}\right) \left(\frac{s}{a}\right).$$

D'un autre côté, on tire de la congruence $\pm t = xs \pmod{a}$ en se rappelant que a est de la forme $4n+1$: $\left(\frac{t}{a}\right) = \left(\frac{x}{a}\right) \left(\frac{s}{a}\right)$. Si l'on multiplie maintenant membre par membre cette équation et la précédente, on aura $\left(\frac{t^2}{a}\right) = \left(\frac{x}{a}\right) \left(\frac{x+\psi}{a}\right) \left(\frac{s^2}{a}\right)$ ou ce qui revient au même: $\left(\frac{x(x+\psi)}{a}\right) = 1$, résultat qui a lieu lorsque a est résidu biquadratique relativement à p . On trouverait de la même manière que, si a n'est pas résidu biquadratique par rapport à p , on a $\left(\frac{x(x+\psi)}{a}\right) = -1$.

Ces résultats sont relatifs au cas où g n'est pas divisible par a . Reste-rait à traiter le cas où g est divisible par a . L'analyse qu'il faut appliquer

à ce second cas, étant entièrement semblable à celle que nous avons exposée avec détail dans ce qui précède, nous nous dispenserons de la développer ici, et nous nous bornerons à énoncer la conclusion à laquelle elle conduit :

„Si g est divisible par a , a est ou n'est pas résidu biquadratique par rapport à p , selon que a est de la forme $8n+1$ ou de celle-ci: $8n+5$.“

Ce résultat et celui qui précède constituent le théorème II énoncé dans le dernier paragraphe du mémoire précédent.

On a sans doute remarqué que les énoncés des théorèmes I et II sont tels qu'il n'y entre que la racine ψ du carré pair ψ^2 que l'on obtient en décomposant p en deux carrés. Il serait facile de modifier ces énoncés de manière à ce qu'ils ne renfermassent plus que la racine g du carré impair. On y parviendrait en suivant une marche entièrement semblable à celle que nous avons exposée dans ce qui précède.

Les résultats (δ') et (θ'), sur lesquels nous nous sommes appuyé pour établir les théorèmes I et II, renferment eux-mêmes une infinité de théorèmes intéressants analogues au premier des théorèmes de M. GAUSS. On déduit, par exemple, de l'énoncé (θ'), en y supposant $a = 5$:

„ p désignant un nombre premier $20n+1$, si l'on fait $p = t^2 + 5u^2$, 5 sera ou ne sera pas résidu biquadratique relativement à p , selon que u est pair ou impair; au contraire, si p désigne un nombre premier $20n+9$ et qu'on fasse de même $p = t^2 + 5u^2$, 5 sera ou ne sera pas résidu biquadratique par rapport à p , selon que u est impair ou pair.“

Les théorèmes (δ') et (θ') se rapportent aux équations :

$$t^2 - bu^2 = ps^2, \quad t^2 + au^2 = ps^2.$$

On trouverait par des considérations du même genre des résultats analogues relatifs aux équations $t^2 + bu^2 = ps^2$, $t^2 - au^2 = ps^2$.

En traitant la première de ces équations et faisant ensuite, pour donner un exemple, $b = 3$, on aurait ce théorème particulier :

„ p désignant un nombre premier $12n+1$, si l'on fait $p = t^2 + 3u^2$, t sera un nombre impair. Cela posé, je dis que 3 sera ou ne sera pas résidu biquadratique par rapport à p , selon que t est de la forme $12n \pm 1$ ou de celle-ci: $12n \pm 5$.“

DÉMONSTRATIONS NOUVELLES DE QUELQUES THÉORÈMES RELATIFS AUX NOMBRES.

PAR

M. G. LEJEUNE DIRICHLET.
PROF. DE MATH.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 3 p. 390—393.

DÉMONSTRATIONS NOUVELLES DE QUELQUES THÉORÈMES RELATIFS AUX NOMBRES.

Parmi les différentes démonstrations que les géomètres ont successivement données du théorème de WILSON, celle que M. GAUSS a exposée dans ses „*Disquisitiones arithmeticae*, art. 77” et qui est fondée sur la considération des nombres correspondants (*numeri socii*), est sans contredit la plus simple. En généralisant un peu la définition des nombres correspondants et en suivant ensuite une marche analogue à celle de M. GAUSS, on peut démontrer simultanément le théorème de WILSON et deux autres propositions qui sont d'un grand usage dans la théorie des nombres. C'est ce que nous allons faire voir en peu de mots.

La lettre p désignant un nombre premier, EULER qui le premier s'est servi de cette considération, nomme correspondants deux nombres m et n , l'un et l'autre moindres que p et tels que leur produit mn donne l'unité pour reste lorsqu'il est divisé par p .

Généralisons cette définition et appelons correspondants deux nombres m et n moindres que p et dont le produit mn donne le même reste qu'un nombre déterminé a que nous supposons n'être pas divisible par p . Cela posé, considérons la suite:

$$(1) \quad 1, 2, 3, \dots, p-1.$$

Il est facile de voir que, si m désigne l'un quelconque des nombres qui composent cette suite, ce nombre m aura son correspondant n et n'en aura qu'un. Cela résulte immédiatement de ce que la congruence $my = a \pmod{p}$, dans laquelle ni m ni a ne sont divisibles par p , a toujours une racine y moindre que p et n'en a qu'une.

Il peut arriver que n soit égal à m . On a alors $m^2 \equiv a \pmod{p}$, ce qui fait voir que ce cas ne peut avoir lieu qu'autant qu'il existe un carré

donnant le même reste que a , ou, en d'autres termes, qu'autant que a est résidu quadratique par rapport à p . Distinguons actuellement deux cas selon que a est ou n'est pas résidu quadratique par rapport à p et commençons par le dernier de ces deux cas.

Soit, dans ce cas, m l'un quelconque des nombres (1) et n son correspondant. On aura $mn \equiv a \pmod{p}$ et n sera différent de m . Après avoir ôté les nombres m, n de la suite (1), il restera $p-3$ nombres. Désignons par m' l'un quelconque de ces $p-3$ nombres restants et par n' son correspondant; n' sera différent de m' et l'on aura $m'n' \equiv a \pmod{p}$. En continuant de procéder ainsi, on épuîsera la suite (1) et l'on formera $\frac{1}{2}(p-1)$ groupes composés chacun de deux nombres correspondants: car chaque nombre n'ayant qu'un correspondant qui est mis de côté en même temps que lui, on ne peut jamais, pour former un nouveau groupe, avoir besoin d'un des nombres déjà mis de côté.

Le produit de deux nombres composant un groupe donnant le même reste que a , et les groupes étant au nombre de $\frac{1}{2}(p-1)$, on voit que le produit des nombres dont l'ensemble des groupes est formé, c'est-à-dire le produit des nombres compris dans la série (1), donne le même reste que le nombre a élevé à la puissance $\frac{1}{2}(p-1)$. On a donc dans le cas que nous venons d'examiner:

$$(2) \quad 1.2.3\dots(p-1) \equiv a^{\frac{1}{2}(p-1)} \pmod{p}.$$

Passons au second cas qui a lieu lorsque a est résidu quadratique de p . Il existe dans ce cas un carré k^2 (dont la racine k peut être supposée $< p$) tel que $k^2 \equiv a \pmod{p}$. Le carré du nombre $p-k$, qui est également moindre que p , donne aussi le même reste que a lorsqu'il est divisé par p . Les nombres k et $p-k$ étant ôtés de la suite (1), il n'y restera aucun nombre x tel que $x^2 \equiv a \pmod{p}$. Car si parmi les nombres restants il y en avait un satisfaisant à cette condition, $x^2 - k^2 = (x+k)(x-k)$ serait divisible par p : il faudrait donc qu'un des facteurs $x+k, x-k$ le fût pareillement; or c'est ce qui est manifestement impossible, x étant plus petit que p et différent de k et $p-k$. — Cela posé, on voit, comme dans le cas déjà examiné, que les $p-3$ nombres qui restent dans la suite (1) après en avoir ôté k et $p-k$, se correspondent deux à deux, d'où l'on conclut comme précédemment que le produit de ces nombres donne le même reste que $a^{\frac{1}{2}(p-3)}$. Il suit de là que le produit de tous les nombres qui composent la suite (1) donne le même reste

que $a^{k(p-k)} \equiv k(p-k)$, et comme, d'après ce qu'on a vu plus haut, on a $k(p-k) \equiv -k^2 \equiv -a \pmod{p}$, il vient ce résultat :

$$1.2.3\dots(p-1) \equiv -a^{\frac{1}{2}(p-1)} \pmod{p}.$$

Ce résultat et celui que nous avons obtenu plus haut, peuvent être réunis dans la formule suivante :

$$(3) \quad 1.2.3\dots(p-1) \equiv \mp a^{\frac{1}{2}(p-1)} \pmod{p},$$

dans laquelle il faut prendre le signe supérieur ou inférieur, selon que le nombre a est ou n'est pas résidu quadratique de p . Si nous posons $a = 1$, le signe supérieur aura lieu, l'unité étant un carré et par conséquent résidu quadratique de tout nombre. Nous avons donc :

$$1.2.3\dots(p-1) \equiv -1 \pmod{p},$$

congruence qui constitue le théorème de WILSON.

Remplaçons le premier membre de la formule (3) par le nombre -1 qui n'en diffère, comme nous venons de le voir, que d'un multiple de p , et changeons ensuite les signes des deux membres; il viendra ainsi :

$$a^{\frac{1}{2}(p-1)} \equiv \pm 1 \pmod{p},$$

congruence dans laquelle il faudra choisir le signe $+$ ou le signe $-$, selon que a est ou n'est pas résidu quadratique de p . Le théorème que cette formule renferme, et qui a été découvert par EULER, est d'une grande importance dans la théorie des résidus. — On fera disparaître le double signe dans la dernière congruence en élevant ses deux membres au carré. On trouve ainsi :

$$a^{p-1} \equiv 1 \pmod{p},$$

ce qui est le théorème de FERMAT.

Ce dernier théorème peut être démontré très simplement de la manière suivante, sans qu'il soit nécessaire de rien supposer de ce qui précède.

Les nombres a et p conservant leur signification, considérons les $p-1$ multiples de a que voici :

$$a, 2a, 3a, \dots, (p-1)a.$$

Il est facile de voir que deux de ces nombres ne sauraient donner le même reste quand on les divise par p ; car si les restes provenant des multiples ma et na étaient égaux, $ma - na = (m-n)a$ serait divisible par p , ce qui est impossible, a n'étant pas divisible par p , et $m-n$ étant $< p$ sans

pouvoir être zéro. Les restes que l'on obtient en divisant par p les $p-1$ multiples de a , étant tous différents entre eux et aucun de ces restes ne pouvant être nul, comme on le voit facilement, ces restes doivent coïncider avec les nombres de la série 1, 2, 3, . . . , $p-1$, quand on fait abstraction de l'ordre dans lequel ils se suivent. Il suit de là que le produit des $p-1$ multiples de a , doit donner le même reste que le produit $1.2.3\dots(p-1)$.

La différence de ces produits est donc un multiple de p . Or cette différence pouvant facilement se mettre sous la forme :

$$(a^{p-1}-1)(1.2.3\dots(p-1))$$

et $1.2.3\dots(p-1)$ n'étant pas divisible par p , on en conclut que $a^{p-1}-1$ est multiple de p , ou, ce qui est la même chose, que a^{p-1} étant divisé par p donne l'unité pour reste.

QUESTION D'ANALYSE INDÉTERMINÉE.

PAR

M. G. LEJEUNE DIRICHLET.
PROF. DE MATH.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 3 p. 407—408.

QUESTION D'ANALYSE INDÉTERMINÉE.

La lettre p désignant un nombre premier impair, on sait, par le théorème de WILSON, que le produit $1.2.3\dots(p-1)$, augmenté de l'unité, est divisible par p . On peut substituer au produit précédent celui que l'on obtient en remplaçant ses $\frac{1}{2}(p-1)$ derniers facteurs qui sont:

$$p-1, \quad p-2, \quad \dots \quad \frac{1}{2}(p+1),$$

par les nombres:

$$-1, \quad -2, \quad \dots \quad -\frac{1}{2}(p-1),$$

qui en diffèrent respectivement de p . On voit ainsi que l'expression:

$$\pm [1.2.3\dots\frac{1}{2}(p-1)]^2 + 1,$$

dans laquelle il faut prendre le signe supérieur ou inférieur, selon que $\frac{1}{2}(p-1)$ est pair ou impair, est toujours un multiple de p . Or $\frac{1}{2}(p-1)$ est pair ou impair, selon que p est de la forme $4n+1$ ou de celle-ci: $4n+3$. On a donc pour tout nombre premier $p = 4n+1$:

$$[1.2.3\dots\frac{1}{2}(p-1)]^2 + 1$$

égal à un multiple de p , et pour tout nombre premier $p = 4n+3$:

$$-[1.2.3\dots\frac{1}{2}(p-1)]^2 + 1,$$

ou ce qui revient au même:

$$[1.2.3\dots\frac{1}{2}(p-1)]^2 - 1$$

égal à un multiple de p .

Ces deux corollaires du théorème de WILSON sont dus à LAGRANGE, qui les a énoncés dans le beau mémoire où il a le premier démontré le théorème qu'on vient de nommer. Le dernier de ces corollaires donne lieu à une question que nous croyons pouvoir proposer à l'attention des géomètres qui s'occupent de la théorie des nombres.

La différence:

$$[1.2.3\dots\frac{1}{2}(p-1)]^2 - 1$$

étant divisible par p (p désignant un nombre premier $4n+3$) et cette différence pouvant se décomposer dans les deux facteurs :

$$1.2.3\dots\frac{1}{2}(p-1)+1, \quad 1.2.3\dots\frac{1}{2}(p-1)-1,$$

il s'ensuit que l'expression :

$$1.2.3\dots\frac{1}{2}(p-1)\pm 1$$

avec le signe convenable est un multiple de p . On demande une règle qui fasse connaître le signe convenable, sans qu'il soit nécessaire de chercher, par des multiplications successives, le reste que l'on obtient en divisant le produit $1.2.3\dots\frac{1}{2}(p-1)$ par p . Il est facile de voir que la question proposée revient à celle de savoir si $1.2.3\dots\frac{1}{2}(p-1)$ est ou n'est pas résidu quadratique de p .

NOTE SUR LES INTÉGRALES DÉFINIES.

PAR

M. G. LEJEUNE DIRICHLET.
PROF. DE MATH.

Crelle, Journal für die reine und angewandte Mathematik. Bd. 4 p. 94--98.

NOTE SUR LES INTÉGRALES DÉFINIES.

Quoique les intégrales qui font l'objet de cette note, soient comprises en grande partie parmi celles dont MM. POISSON et CAUCHY et d'autres savants ont déterminé les valeurs dans ces derniers temps, je me flatte que cette nouvelle manière d'y parvenir pourra intéresser les géomètres par son extrême simplicité. Le procédé dont je fais usage, est fondé sur la propriété connue des intégrales doubles, d'être indépendantes de l'ordre dans lequel les deux intégrations sont effectuées. C'est une extension de la méthode dont MM. LAPLACE et POISSON ont fait un emploi si heureux dans la théorie des intégrales définies. Mais si l'on doit convenir que la méthode dont il s'agit a acquis son importance principale par les applications ingénieuses que les géomètres cités en ont faites, la justice exige aussi d'attribuer à EULER la première idée de faire servir la propriété énoncée des intégrales doubles à l'évaluation des intégrales définies simples*).

Si l'on désigne par k et m deux constantes positives, et que l'on adopte la notation de M. LEGENDRE, on aura par le simple changement de ky en y :

$$(1) \quad \int_0^{\infty} e^{-ky} y^{m-1} dy = \frac{\int_0^{\infty} e^{-y} y^{m-1} dy}{k^m} = \frac{\Gamma(m)}{k^m},$$

les limites étant zéro et l'infini positif. EULER a été conduit par l'induction à remplacer la constante réelle k par une quantité de la forme $k + \theta\sqrt{-1}$, la partie réelle étant toujours positive, sans quoi l'intégrale deviendrait infinie. Il a obtenu de cette manière l'équation suivante:

$$\int_0^{\infty} e^{-(k+\theta\sqrt{-1})y} y^{m-1} dy = \frac{\Gamma(m)}{(k+\theta\sqrt{-1})^m},$$

* *Novi Comment. acad. Petrop. tom. XVI.*

qui a été vérifiée depuis par M. POISSON*). L'équation précédente a non seulement lieu pour des valeurs réelles et positives de m , mais elle subsiste encore quand même m serait imaginaire, pourvu qu'alors la partie réelle de m fût toujours positive. C'est ce qu'on peut démontrer facilement par le même procédé qui a servi à la vérifier dans le cas de m réelle. Si donc nous désignons par p une quantité soumise à la seule restriction d'avoir sa partie réelle positive, nous avons :

$$(2) \quad \int_0^{\infty} e^{-(k+\theta l-1)y} y^{p-1} dy = \frac{\Gamma(p)}{(k+\theta l-1)^p}.$$

Si l'on remplace dans cette dernière formule la quantité réelle quelconque θ par $x+l$, x et l étant des quantités réelles quelconques, et qu'on écrive ensuite simplement k à la place de $k+l-1$, il viendra celle-ci :

$$(3) \quad \int_0^{\infty} e^{-(k+x l-1)y} y^{p-1} dy = \frac{\Gamma(p)}{(k+x l-1)^p}.$$

où x désigne une quantité réelle et k et p sont deux quantités soumises à la restriction d'avoir leurs parties réelles positives.

Outre la formule précédente, nous aurons encore besoin d'une autre formule dont on est redevable à M. LAPLACE. La constante α étant réelle et positive et b désignant une quantité soumise à la restriction d'avoir sa partie réelle positive, la formule dont nous parlons, est celle-ci :

$$\int_{-\infty}^{\infty} \frac{b^2+x^2}{\cos \alpha x} dx = \frac{\pi}{b} e^{-\alpha b}.$$

Nous l'écrirons d'une manière un peu différente, en remplaçant $\cos \alpha x$ par $e^{-x l-1}$, ce qui est permis, l'intégrale $\int_{-\infty}^{\infty} \frac{b^2+x^2}{\sin \alpha x} dx$, qui est composée d'éléments égaux deux à deux, mais de signes opposés, étant évidemment nulle. Nous

* Pour éviter toute ambiguïté, il convient de fixer le sens de quelques signes. Les lettres k et l désignent deux quantités réelles et la première de plus positive, la notation $l(k+\theta l-1)$ servira à remplacer l'expression $l(x+\theta l-1)$, x étant la quantité positive $\sqrt{(k^2+\theta^2)}$ et θ l'arc compris entre $-\frac{\pi}{2}$ et $\frac{\pi}{2}$ déterminé par l'équation $\operatorname{tg} \theta = \frac{l}{k}$. Les suppositions précédentes étant conservées, et q désignant une quantité quelconque réelle ou imaginaire, $(k+\theta l-1)^q$ indiquera la quantité $e^{q l(k+\theta l-1)} = e^{q l(x+\theta l-1)}$. En vérifiant l'équation (2), on trouve que cette équation n'a lieu qu'autant qu'on attache à la notation $(k+\theta l-1)^p$ le sens que je viens de définir.

avons donc :

$$(4) \quad \int_{-\infty}^{\infty} \frac{e^{-ax}\sqrt{-1}}{b^2+x^2} dx = \frac{\pi}{b} e^{-ba}.$$

L'équation (3) subsistant pour toutes les valeurs réelles de x , on peut intégrer ses deux membres par rapport à cette quantité entre des limites quelconques, après les avoir multipliés par dx et par une fonction quelconque de x . Si l'on multiplie les deux membres par $\frac{e^{-cx}\sqrt{-1}}{b^2+x^2} dx$ (c étant réelle et positive et b conservant sa signification précédente) et qu'on intègre ensuite depuis $x = -\infty$ jusqu'à $x = \infty$, on aura :

$$\int_0^{\infty} e^{-ky} y^{p-1} \left(\int_{-\infty}^{\infty} \frac{e^{-(c+y)x}\sqrt{-1}}{b^2+x^2} dx \right) dy = \Gamma(p) \int_{-\infty}^{\infty} \frac{e^{-cx}\sqrt{-1}}{(k+cx)\sqrt{-1}} \cdot \frac{dx}{b^2+x^2}.$$

Comme $c+y$ est positive (y ne devant recevoir que des valeurs positives dans l'intégration relative à cette variable), on aura en vertu de la formule (4) :

$$\int_{-\infty}^{\infty} \frac{e^{-(c+y)x}\sqrt{-1}}{b^2+x^2} dx = \frac{\pi}{b} e^{-bc} e^{-by}.$$

La substitution de cette valeur dans le premier membre le réduira à la quantité :

$$\frac{\pi e^{-bc}}{b} \int_0^{\infty} e^{-(b+k)y} y^{p-1} dy,$$

ou ce qui est la même chose d'après l'équation (2), la partie réelle de $b+k$ étant évidemment positive :

$$\frac{\pi \Gamma(p) e^{-bc}}{b(b+k)^p}.$$

Égalant cette quantité au second membre et effaçant le facteur $\Gamma(p)$ qui se trouvera commun aux deux membres, on aura définitivement :

$$(5) \quad \int_{-\infty}^{\infty} \frac{e^{-cx}\sqrt{-1}}{(k+cx)\sqrt{-1}} \cdot \frac{dx}{b^2+x^2} = \frac{\pi e^{-bc}}{b(b+k)^p}.$$

En particulierisant les constantes de cette formule, on obtiendra toutes celles dont il est question dans le Mémoire sur les intégrales définies que M. Poisson a inséré dans le 18^{ième} cahier du Journal de l'École Polytechnique.

J'accentue maintenant les lettres k' et p dans l'équation (3), je multiplie ses deux membres par la quantité qui se trouve sous le signe f dans la formule (5) et je les intègre ensuite depuis $x = -\infty$ jusqu'à $x = \infty$.

On effectuera la double intégration comme on l'a fait pour obtenir l'équation (5) avec la seule différence qu'au lieu de s'appuyer sur la formule (4), il faudra s'appuyer sur l'équation (5).

Tout calcul fait, on trouvera:

$$\int_{-\infty}^{+\infty} \frac{e^{-cx}\sqrt{-1}}{b^2+x^2} \cdot \frac{1}{(k+x\sqrt{-1})^p} \cdot \frac{1}{(k'+x\sqrt{-1})^{p'}} dx = \frac{\pi e^{-bc}}{b} \cdot \frac{1}{(b+k)^p} \cdot \frac{1}{(b+k')^{p'}}.$$

En continuant de procéder ainsi, on arrivera à cette formule:

$$(6) \quad \left\{ \begin{aligned} & \int_{-\infty}^{+\infty} \frac{e^{-cx}\sqrt{-1}}{b^2+x^2} \cdot \frac{1}{(k+x\sqrt{-1})^p} \cdot \frac{1}{(k'+x\sqrt{-1})^{p'}} \cdot \frac{1}{(k''+x\sqrt{-1})^{p''}} \dots dx \\ & = \frac{\pi e^{-bc}}{b} \cdot \frac{1}{(b+k)^p} \cdot \frac{1}{(b+k')^{p'}} \cdot \frac{1}{(b+k'')^{p''}} \dots \end{aligned} \right.$$

dans laquelle les facteurs:

$$\frac{1}{(k+x\sqrt{-1})^p} \cdot \frac{1}{(k'+x\sqrt{-1})^{p'}} \cdot \frac{1}{(k''+x\sqrt{-1})^{p''}} \cdot \dots$$

sont en nombre quelconque. Il faut se rappeler que c désigne une quantité positive et que b , k , p , k' , p' , k'' , p'' , ... ou du moins les parties réelles de ces quantités sont également positives.

La formule (6) fournit un grand nombre de conséquences: je me contenterai d'en indiquer une seule.

Si l'on désigne par h une quantité positive supérieure à l'unité, ou une quantité imaginaire ayant pour partie réelle une telle quantité, et par x une quantité réelle quelconque, la partie réelle de la quantité $l(h+x\sqrt{-1})$ sera positive*). On pourra par conséquent la mettre à la place de $k+\theta\sqrt{-1}$ dans la formule (2). On aura ainsi, en remplaçant de plus p par q (q étant une quantité du même genre, c'est-à-dire soumise aux mêmes restrictions que p):

*) Soit $h = m+n\sqrt{-1}$, m et n étant réelles et m de plus positive et > 1 , la partie réelle de $l(h+x\sqrt{-1})$ ou ce qui revient au même, de $l[m+(n+x)\sqrt{-1}]$ sera $\frac{1}{2}l[m^2+(n+x)^2]$, valeur qui sera toujours positive, attendu que la quantité $m^2+(n+x)^2$ ne pourra jamais s'abaisser au-dessous de la quantité positive m^2 , et à fortiori pas au dessous de l'unité, m étant > 1 .

$$(7) \quad \int_0^{\infty} e^{-y^{q/(h+x\sqrt{-1})}} y^{q-1} dy = \frac{\Gamma(q)}{[l(h+x\sqrt{-1})]^q}.$$

ou si l'on écrit simplement $\frac{1}{(h+x\sqrt{-1})^q}$ à la place de $e^{-y^{q/(h+x\sqrt{-1})}}$:

$$\int_0^{\infty} \frac{y^{q-1}}{(h+x\sqrt{-1})^q} dy = \frac{\Gamma(q)}{[l(h+x\sqrt{-1})]^q}.$$

Je multiplie les deux membres de cette dernière équation par la quantité qui se trouve sous le signe f dans l'équation (6) et je les intègre ensuite depuis $x = -\infty$ jusqu'à $x = \infty$:

$$\begin{aligned} & \int_0^{\infty} y^{q-1} dy \left(\int_{-\infty}^{+\infty} \frac{e^{-cx\sqrt{-1}}}{b^2+x^2} \cdot \frac{1}{(h+x\sqrt{-1})^p} \cdot \frac{1}{(k+x\sqrt{-1})^p} \cdot \frac{1}{(k'+x\sqrt{-1})^p} \cdots dx \right) \\ &= \Gamma(q) \int_{-\infty}^{+\infty} \frac{e^{-cx\sqrt{-1}}}{b^2+x^2} \left(\frac{1}{(h+x\sqrt{-1})^p} \cdot \frac{1}{(k+x\sqrt{-1})^p} \cdots \right) \frac{dx}{[l(h+x\sqrt{-1})]^q}. \end{aligned}$$

L'intégrale relative à x du premier membre s'obtient au moyen de la formule (6), y étant positive. En l'effectuant, le premier membre se réduira à:

$$\frac{\pi e^{-hr}}{b} \cdot \frac{1}{(b+h)^p} \cdot \frac{1}{(b+k)^p} \cdot \frac{1}{(b+k')^p} \cdots \int_0^{\infty} \frac{y^{q-1}}{(b+h)^p} dy.$$

Si l'on met dans cette quantité à la place de l'intégrale sa valeur:

$$\frac{\Gamma(q)}{[l(b+h)]^q},$$

qu'on l'égalé au second membre de l'équation précédente et qu'on efface le facteur commun $\Gamma(q)$, on aura:

$$(8) \quad \left\{ \begin{aligned} & \int_{-\infty}^{+\infty} \frac{e^{-cx\sqrt{-1}}}{b^2+x^2} \left(\frac{1}{(h+x\sqrt{-1})^p} \cdot \frac{1}{(k+x\sqrt{-1})^p} \cdots \right) \frac{dx}{[l(h+x\sqrt{-1})]^q} \\ &= \frac{\pi e^{-bc}}{b} \left(\frac{1}{(b+h)^p} \cdot \frac{1}{(b+k)^p} \cdots \right) \frac{1}{[l(b+h)]^q}. \end{aligned} \right.$$

Si l'on accentue les lettres h et q dans la formule (7), qu'on multiplie les deux membres par la quantité qui se trouve sous le signe f dans l'équation (8) et qu'on les intègre ensuite depuis $x = -\infty$ jusqu'à $x = \infty$, on arrivera à une formule semblable à la formule (8), dans laquelle il y aura sous le signe f deux facteurs de la forme:

$$\frac{1}{[l(h+x\sqrt{-1})]^q} \cdot \frac{1}{[l(h'+x\sqrt{-1})]^{q'}}.$$

On pourra introduire de cette manière un nombre quelconque de ces facteurs, ce qui donnera la formule

$$(9) \quad \left\{ \int_{-\infty}^{\infty} \frac{e^{-cx} \sqrt{-1}}{b^2+x^2} \left(\frac{1}{(k+x)\sqrt{-1}} \cdot \frac{1}{(k'+x)\sqrt{-1}} \cdots \right) \left(\frac{1}{[l(h+x)\sqrt{-1}]^q} \cdot \frac{1}{[l(h'+x)\sqrt{-1}]^{q'}} \cdots \right) dx \right. \\ \left. = \frac{\pi e^{-bc}}{b} \left(\frac{1}{(b+k)^p} \cdot \frac{1}{(b+k')^{p'}} \cdots \right) \left(\frac{1}{[l(b+k)]^q} \cdot \frac{1}{[l(b+k')]^{q'}} \cdots \right) \right.$$

dans laquelle on suppose c positive, les parties réelles des quantités b ; k , k' , k'' , ...; p , p' , p'' , ...; q , q' , q'' , ...; h , h' , h'' , ... également positives, et en outre les parties réelles des quantités de la dernière série h , h' , h'' , ... supérieures à l'unité.

SUR LA CONVERGENCE DES SÉRIES TRIGONO-
MÉTRIQUES QUI SERVENT A REPRÉSENTER
UNE FONCTION ARBITRAIRE ENTRE DES
LIMITES DONNÉES.

PAR

M. G. LEJEUNE DIRICHLÉT,

PROF. DE MATH.

SUR LA CONVERGENCE DES SÉRIES TRIGONOMÉTRIQUES QUI SERVENT A REPRÉSENTER UNE FONCTION ARBITRAIRE ENTRE DES LIMITES DONNÉES.

Les séries de sinus et de cosinus, au moyen desquelles on peut représenter une fonction arbitraire dans un intervalle donné, jouissent entre autres propriétés remarquables de celle d'être convergentes. Cette propriété n'avait pas échappé au géomètre illustre qui a ouvert une nouvelle carrière aux applications de l'analyse, en y introduisant la manière d'exprimer les fonctions arbitraires dont il est question; elle se trouve énoncée dans le Mémoire qui contient ses premières recherches sur la chaleur. Mais personne, que je sache, n'en a donné jusqu'à présent une démonstration générale. Je ne connais sur cet objet qu'un travail dû à M. CAUCHY et qui fait partie des Mémoires de l'Académie des sciences de Paris pour l'année 1823. L'auteur de ce travail avoue lui-même que sa démonstration se trouve en défaut pour certaines fonctions pour lesquelles la convergence est pourtant incontestable. Un examen attentif du Mémoire cité m'a porté à croire que la démonstration qui y est exposée n'est pas même suffisante pour les cas auxquels l'auteur la croit applicable. Je vais, avant d'entrer en matière, énoncer en peu de mots les objections auxquelles la démonstration de M. CAUCHY me paraît sujette. La marche que ce géomètre célèbre suit dans cette recherche, exige que l'on considère les valeurs que la fonction $\varphi(x)$ qu'il s'agit de développer, obtient, lorsqu'on y remplace la variable x par une quantité de la forme $u+r\sqrt{-1}$. La considération de ces valeurs semble étrangère à la question et l'on ne voit d'ailleurs pas bien ce que l'on doit entendre par le résultat d'une pareille substitution lorsque la fonction dans laquelle elle a lieu, ne peut pas être exprimée par une formule analytique. Je présente cette objection avec d'autant plus de confiance, que l'auteur me semble partager mon opinion sur ce point. Il insiste en effet dans plusieurs de ses ouvrages sur la nécessité de définir

d'une manière précise le sens que l'on attache à une pareille substitution même lorsqu'elle est faite dans une fonction d'une loi analytique régulière; on trouve surtout dans le Mémoire qu'il a inséré dans le 19^{ième} cahier du Journal de l'École Polytechnique pag. 567 et suiv., des remarques sur les difficultés que font naître les quantités imaginaires placées sous des signes de fonctions arbitraires. Quoi qu'il en soit de cette première observation, la démonstration de M. CAUCHY donne encore lieu à une autre objection qui paraît ne laisser aucun doute sur son insuffisance. La considération des quantités imaginaires conduit l'auteur à un résultat sur le décroissement des termes de la série, qui est loin de prouver que ces termes forment une suite convergente. Le résultat dont il s'agit peut être énoncé comme il suit, en supposant que l'intervalle considéré s'étend depuis zéro jusqu'à 2π .

„Le rapport du terme dont le rang est n , à la quantité $A \frac{\sin nx}{n}$ (A désignant une constante déterminée, dépendante des valeurs extrêmes de la fonction) diffère de l'unité prise positivement d'une quantité qui diminue indéfiniment, à mesure que n devient plus grand.“

De ce résultat et de ce que la série qui a $A \frac{\sin nx}{n}$ pour terme général, est convergente, l'auteur conclut que la série trigonométrique générale l'est également. Mais cette conclusion n'est pas permise, car il est facile de s'assurer que deux séries (du moins lorsque, comme il arrive ici, les termes n'ont pas tous le même signe) peuvent être l'une convergente, l'autre divergente, quoique le rapport de deux termes de même rang diffère aussi peu que l'on veut de l'unité prise positivement lorsque les termes sont d'un rang très avancé.

On en voit un exemple très simple dans les deux séries, ayant l'une pour terme général $\frac{(-1)^n}{\sqrt{n}}$, et l'autre $\frac{(-1)^n}{\sqrt{n}} \left(1 + \frac{(-1)^n}{\sqrt{n}}\right)$. La première de ces séries est convergente, la seconde au contraire est divergente, car en la soustrayant de la première on obtient la série divergente:

$$-1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{4} - \frac{1}{5} - \text{etc.}$$

et cependant le rapport de deux termes correspondants, qui est $1 \pm \frac{1}{\sqrt{n}}$, converge vers l'unité à mesure que n croît.

Je vais maintenant entrer en matière, en commençant par l'examen des cas les plus simples, auxquels tous les autres peuvent être ramenés. Désignons

par h un nombre positif inférieur ou tout au plus égal à $\frac{\pi}{2}$ et par $f(\beta)$ une fonction de β qui reste continue entre les limites 0 et h ; j'entends par là une fonction qui a une valeur finie et déterminée pour toute valeur de β comprise entre 0 et h , et en outre telle que la différence $f(\beta+\epsilon)-f(\beta)$ diminue sans limite lorsque ϵ devient de plus en plus petit. Supposons encore que la fonction reste toujours positive entre les limites 0 et h et qu'elle décroisse constamment depuis 0 jusqu'à h , en sorte que si p et q désignent deux nombres compris entre 0 et h , $f(p)-f(q)$ ait toujours un signe opposé à celui de $p-q$. Cela posé, considérons l'intégrale:

$$(1) \quad \int_0^h \frac{\sin i\beta}{\sin \beta} f(\beta) d\beta$$

dans laquelle i est une quantité positive, et voyons ce que cette intégrale deviendra à mesure que i croit. Pour cela partageons-la en plusieurs autres prises la première depuis $\beta = 0$ jusqu'à $\beta = \frac{\pi}{i}$, la seconde depuis $\beta = \frac{\pi}{i}$ jusqu'à $\beta = \frac{2\pi}{i}$, et ainsi de suite, l'avant-dernière ayant pour limites $(r-1)\frac{\pi}{i}$ et $\frac{r\pi}{i}$, et la dernière $\frac{r\pi}{i}$ et h , $\frac{r\pi}{i}$ désignant le plus grand multiple de $\frac{\pi}{i}$ qui soit contenu dans h . Il est facile de voir que ces intégrales nouvelles, dont le nombre est $r+1$, sont alternativement positives et négatives, la fonction placée sous le signe d'intégration étant évidemment toujours positive entre les limites de la première, négative entre les limites de la seconde et ainsi de suite. Il n'est pas moins facile de se convaincre que chacune d'elles est plus petite que la précédente, abstraction faite du signe. En effet ν désignant un entier $< r$, les expressions:

$$\int_{(\nu-1)\frac{\pi}{i}}^{\frac{\nu\pi}{i}} \frac{\sin i\beta}{\sin \beta} f(\beta) d\beta \quad \text{et} \quad \int_{\frac{\nu\pi}{i}}^{(\nu+1)\frac{\pi}{i}} \frac{\sin i\beta}{\sin \beta} f(\beta) d\beta$$

représentent deux intégrales consécutives. Remplaçons dans la seconde β par $\frac{\pi}{i} + \beta$; elle se changera ainsi en celle-ci:

$$\int_{(\nu-1)\frac{\pi}{i}}^{\frac{\nu\pi}{i}} \frac{\sin(i\beta + \pi)}{\sin\left(\beta + \frac{\pi}{i}\right)} f\left(\beta + \frac{\pi}{i}\right) d\beta$$

ou ce qui revient au même:

$$-\int_{\frac{\nu-1}{i}\pi}^{\frac{\nu\pi}{i}} \frac{\sin i\beta}{\sin\left(\beta+\frac{\pi}{i}\right)} f\left(\beta+\frac{\pi}{i}\right) d\beta.$$

Les deux intégrales qu'il s'agit de comparer ayant ainsi les mêmes limites, on voit sans peine que la seconde a une valeur numérique inférieure à celle de la première. Il suffit pour cela de remarquer qu'il suit de la supposition faite sur la fonction $f(\beta)$:

$$f\left(\frac{\pi}{i} + \beta\right) < f(\beta),$$

et que d'un autre côté:

$$\sin\left(\frac{\pi}{i} + \beta\right) > \sin\beta,$$

les arcs β et $\frac{\pi}{i} + \beta$ étant l'un et l'autre moindres que $\frac{\pi}{2}$, car il en résulte l'inégalité:

$$\frac{f(\beta)}{\sin\beta} > \frac{f\left(\beta+\frac{\pi}{i}\right)}{\sin\left(\beta+\frac{\pi}{i}\right)},$$

qui ayant lieu pour toutes les valeurs de β intermédiaires entre les limites $(\nu-1)\frac{\pi}{i}$ et $\frac{\nu\pi}{i}$, fait voir, comme nous l'avons dit, que chaque intégrale est plus grande que celle qui la suit, abstraction faite du signe. Cette circonstance a lieu à fortiori, lorsqu'on compare l'avant-dernière à la dernière, attendu que la différence des limites $\frac{\nu\pi}{i}$ et h de la dernière est inférieure à $\frac{\pi}{i}$, différence commune des limites de toutes les autres.

Examinons actuellement un peu plus en détail l'intégrale du rang ν , qui est:

$$\int_{\frac{\nu-1}{i}\pi}^{\frac{\nu\pi}{i}} \frac{\sin i\beta}{\sin\beta} f(\beta) d\beta.$$

Comme la fonction de β qui se trouve sous le signe f est le produit des facteurs $\frac{\sin i\beta}{\sin\beta}$ et $f(\beta)$, qui sont l'un et l'autre des fonctions continues de

β entre les limites de l'intégration, et comme d'un autre côté le premier de ces facteurs conserve toujours le même signe entre ces mêmes limites, on conclura, en vertu d'un théorème connu, que l'intégrale considérée est égale à l'intégrale du premier facteur multipliée par une quantité comprise entre la valeur la plus grande et la valeur la plus petite de l'autre facteur. Le second facteur décroissant depuis la première limite jusqu'à la seconde, la quantité dont il s'agit est comprise entre $f\left(\frac{(v-1)\pi}{i}\right)$ et $f\left(\frac{v\pi}{i}\right)$. En la désignant par q_v , notre intégrale sera équivalente à :

$$q_v \int_{\frac{(v-1)\pi}{i}}^{\frac{v\pi}{i}} \frac{\sin i\beta}{\gamma \sin \beta} d\beta.$$

L'intégrale que renferme encore cette expression, dépend à la fois de v et de i . Elle est positive ou négative selon que $v-1$ est pair ou impair: nous la désignerons désormais par K_v , abstraction faite du signe. Nous aurons bientôt besoin de connaître la limite vers laquelle elle converge, lorsque, v restant invariable, i devient de plus en plus grand. Pour découvrir cette limite, remplaçons β par $\frac{\gamma}{i}$, γ étant une nouvelle variable. Nous aurons ainsi:

$$\int_{(v-1)\pi}^{v\pi} \frac{\sin \gamma}{i \sin\left(\frac{\gamma}{i}\right)} d\gamma.$$

Sous cette forme, il est évident qu'elle converge vers la limite:

$$\int_{(v-1)\pi}^{v\pi} \frac{\sin \gamma}{\gamma} d\gamma.$$

que pour abrégé nous désignerons par k_v , abstraction faite du signe.

On sait que l'intégrale $\int_0^\pi \frac{\sin \gamma}{\gamma} d\gamma$ a une valeur finie et égale à $\frac{\pi}{2}$. Cette intégrale peut être partagée en une infinité d'autres, prises la première depuis $\gamma = 0$ jusqu'à $\gamma = \pi$, la seconde depuis $\gamma = \pi$ jusqu'à $\gamma = 2\pi$, et ainsi de suite. Ces nouvelles intégrales sont alternativement positives et négatives, chacune d'elles a une valeur numérique inférieure à celle de la précédente, et celle du rang v est k_v , abstraction faite du signe. La proposition qu'on vient de citer, revient donc à dire que la suite infinie:

$$(2) \quad k_1 - k_2 + k_3 - k_4 + k_5 - \text{etc.}$$

est convergente et a une somme égale à $\frac{\pi}{2}$.

Les termes de cette suite allant toujours en décroissant, il suit d'une proposition connue que la somme des n premiers termes est supérieure ou inférieure à $\frac{\pi}{2}$, selon que n est impair ou pair, et que cette somme qu'on peut désigner par S_n , diffère de $\frac{\pi}{2}$ d'une quantité moindre que le terme suivant k_{n+1} .

Reprenons actuellement l'intégrale (1) et cherchons à déterminer la limite vers laquelle elle converge lorsque i croît indéfiniment. En faisant ainsi croître le nombre i , les intégrales dans lesquelles nous avons décomposé l'intégrale (1), changeront sans cesse de valeur en même temps que leur nombre augmentera: il s'agit de connaître le résultat de ce double changement lorsqu'il continue indéfiniment. Pour cela, prenons un nombre entier m (qu'il soit supposé pair pour plus de simplicité) et supposons que le nombre m reste invariable pendant que i croît. Le nombre r , qui croît sans cesse avec i , finira bientôt par surpasser le nombre invariable m , quelque grand qu'on l'ait choisi.

Cela posé, partageons en deux groupes les intégrales dont la somme est équivalente à l'intégrale (1). Le premier groupe comprendra les m premières de ces intégrales, et le second sera composé de toutes les suivantes. On aura pour la somme du premier groupe:

$$(3) \quad K_1 e_1 - K_2 e_2 + K_3 e_3 - K_4 e_4 + \dots - K_m e_m$$

et le second, dont le nombre des termes croît sans cesse avec i , a pour premiers termes:

$$(4) \quad K_{m+1} e_{m+1} - K_{m+2} e_{m+2} + \dots$$

Considérons séparément ces deux groupes. Le nombre i croissant indéfiniment, la somme (3) convergera vers une limite qu'il est facile de déterminer. En effet, les quantités q_1, q_2, \dots, q_m qui sont comprises la première entre $f(0)$ et $f\left(\frac{\pi}{i}\right)$, la seconde entre $f\left(\frac{\pi}{i}\right)$ et $f\left(\frac{2\pi}{i}\right)$, et la dernière entre $f\left(\frac{(m-1)\pi}{i}\right)$ et $f\left(\frac{m\pi}{i}\right)$ convergent chacune vers la limite $f(0)$, lorsque m restant invariable, i croît sans cesse. D'un autre côté nous avons vu que les quantités:

$$K_1, K_2, \dots, K_m$$

convergent dans les mêmes circonstances respectivement vers les limites:

$$k_1, k_2, \dots, k_m.$$

Donc la somme (3) converge vers la limite:

$$(k_1 - k_2 + k_3 - \dots - k_m) f(0) = S_m f(0),$$

ce qui veut dire que la différence entre la somme (3) et $S_m f(0)$ finira toujours, abstraction faite du signe, par être constamment inférieure à ω . ω désignant une quantité positive aussi petite que l'on veut.

Considérons pareillement la somme (4), dont le nombre des termes augmente sans cesse. Ses termes étant alternativement positifs et négatifs, et chacun d'eux ayant une valeur numérique inférieure à celle du terme précédent, comme nous l'avons vu plus haut, en considérant les intégrales que ces termes représentent, il suit d'un principe connu*) que cette somme, quel que soit le nombre de ses termes, est positive comme son premier terme $K_{m+1} q_{m+1}$ et a une valeur inférieure à celle de ce terme. Or ce premier terme convergeant vers la limite $k_{m+1} f(0)$, il s'ensuit que la somme (4) finira toujours par être inférieure à $k_{m+1} f(0)$ augmenté d'une quantité positive ω' aussi petite que l'on veut. En combinant ce résultat avec celui que nous avons obtenu sur la somme (3), il n'y a qu'un instant, on verra que l'intégrale (1) qui est la somme des expressions (3) et (4) finira toujours par différer de $S_m f(0)$ d'une quantité moindre, abstraction faite du signe, que $\omega + \omega' + k_{m+1} f(0)$, ω et ω' étant deux nombres d'une petitesse arbitraire. D'un autre côté S_m diffère de $\frac{\pi}{2}$ d'une quantité numériquement inférieure à k_{m+1} ; donc l'intégrale finira toujours par différer de $\frac{\pi}{2} f(0)$ d'une quantité moindre que $\omega + \omega' + 2k_{m+1} f(0)$, abstraction faite du signe.

Comme m peut être choisi tellement grand que k_{m+1} soit moindre que toute grandeur donnée, il s'ensuit que l'intégrale (1) finira toujours, lorsque i croît sans limite, par différer constamment de $\frac{\pi}{2} f(0)$ d'une quantité moindre, abstraction faite du signe, qu'un nombre aussi petit que l'on veut. Il est ainsi

*) Le principe sur lequel nous nous appuyons peut être énoncé de cette manière.

Les lettres A, A', A'', \dots désignant des quantités positives en nombre quelconque et telles que:

$$A > A' > A'' > \text{etc.},$$

la quantité:

$$A - A' + A'' - A''' + \text{etc.}$$

est positive et inférieure à A . Cela résulte immédiatement de ce que la quantité précédente peut être mise sous l'une et l'autre de ces deux formes:

$$(A - A') + (A'' - A''') + \text{etc.},$$

$$A - (A' - A'') - (A''' - A^{IV}) - \text{etc.}$$

prouvé, que l'intégrale (1) converge vers la limite $\frac{\pi}{2}f(0)$ pour des valeurs croissantes de i .

Supposons maintenant que la fonction $f(\beta)$, au lieu d'être toujours décroissante depuis 0 jusqu'à h , soit constante et égale à l'unité. On pourra dans ce cas déterminer la limite vers laquelle converge l'intégrale (1) par les mêmes considérations que nous venons d'employer; c'est ce qu'on voit tout de suite, en se rappelant que la démonstration précédente est fondée sur ce que les intégrales, dans lesquelles nous avons décomposé l'intégrale (1), forment une suite décroissante. Or ce décroissement tient à deux choses, au décroissement du facteur $f(\beta)$ et à l'accroissement du diviseur $\sin\beta$. Si $f(\beta)$ devient un nombre constant, l'accroissement de $\sin\beta$ suffira toujours pour rendre chaque intégrale de la série plus petite que la précédente. On trouvera ainsi, en supposant toujours h positive et tout au plus égale à $\frac{\pi}{2}$, que l'intégrale $\int_0^h \frac{\sin i\beta}{\sin\beta} d\beta$ converge vers la limite $\frac{\pi}{2}$. Il suit de là que l'intégrale $\int_0^h c \frac{\sin i\beta}{\sin\beta} d\beta$, dans laquelle c est une constante positive ou négative, converge vers la limite $c \frac{\pi}{2}$.

Nous avons supposé que la fonction $f(\beta)$ était décroissante et positive entre les limites 0 et h . La première circonstance ayant toujours lieu, c'est-à-dire la fonction étant telle que $f(p) - f(q)$ ait un signe contraire à celui de $p - q$ pour des valeurs p et q comprises entre 0 et h , supposons que $f(\beta)$ ne soit pas toujours positive. On prendra alors une constante positive c assez grande pour que $c + f(\beta)$ conserve toujours un signe positif depuis $\beta = 0$ jusqu'à $\beta = h$. L'intégrale $\int_0^h f(\beta) \frac{\sin i\beta}{\sin\beta} d\beta$ étant égale à la différence de celles-ci:

$$\int_0^h [c + f(\beta)] \frac{\sin i\beta}{\sin\beta} d\beta \quad \text{et} \quad \int_0^h c \frac{\sin i\beta}{\sin\beta} d\beta.$$

sa limite sera la différence des limites vers lesquelles convergent ces dernières. Or ces dernières rentrent dans les cas précédemment examinés ($c + f(\beta)$ étant une fonction décroissante et positive) et convergent vers les limites $[c + f(0)] \frac{\pi}{2}$ et $c \frac{\pi}{2}$, d'où il suit que la première converge vers la limite $\frac{\pi}{2}f(0)$.

Considérons actuellement une fonction $f(\beta)$ croissante depuis 0 jusqu'à h . Dans ce cas $-f(\beta)$ sera une fonction décroissante. L'intégrale

$\int_0^h -f(\beta) \frac{\sin i\beta}{\sin \beta} d\beta$ convergera donc vers la limite $-\frac{\pi}{2}f(0)$, et par conséquent l'intégrale $\int_0^h f(\beta) \frac{\sin i\beta}{\sin \beta} d\beta$ vers la limite $\frac{\pi}{2}f(0)$.

En réunissant ces résultats, on aura cet énoncé:

(5) $\left\{ \begin{array}{l} \text{«Quelle que soit la fonction } f(\beta), \text{ pourvu qu'elle reste continue entre} \\ \text{les limites } 0 \text{ et } h \text{ (} h \text{ étant positive et tout au plus égale à } \frac{\pi}{2} \text{), et} \\ \text{qu'elle croisse ou qu'elle décroisse depuis la première de ces limites} \\ \text{jusqu'à la seconde, l'intégrale } \int_0^h f(\beta) \frac{\sin i\beta}{\sin \beta} d\beta \text{ finira par différer con-} \\ \text{stantment de } \frac{\pi}{2}f(0) \text{ d'une quantité moindre que tout nombre as-} \\ \text{signable, lorsqu'on y fait croître } i \text{ au delà de toute limite positive.} \text{»}$

Désignons par g un nombre positif différent de zéro et inférieur à h , et supposons que la fonction reste continue et croisse ou décroisse depuis g jusqu'à h . L'intégrale $\int_g^h f(\beta) \frac{\sin i\beta}{\sin \beta} d\beta$ convergera alors vers une limite qu'il est facile de découvrir. On pourrait y parvenir par des considérations analogues à celles que nous avons appliquées à l'intégrale (1); mais il est plus simple de ramener ce nouveau cas à ceux que nous avons considérés dans ce qui précède. La fonction n'étant donnée que depuis g jusqu'à h , reste entièrement arbitraire pour les valeurs de β comprises entre 0 et g . Supposons que l'on entende par $f(\beta)$, pour les valeurs de β comprises entre 0 et g , une fonction continue et croissante ou décroissante depuis 0 jusqu'à g , selon que $f(\beta)$ croît ou décroît depuis g jusqu'à h : supposons encore que $f(g-\epsilon)$ diffère infiniment peu de $f(g+\epsilon)$, si ϵ décroît sans limite; ayant satisfait d'une manière quelconque à ces conditions, ce qu'on peut toujours faire d'une infinité de manières, la fonction $f(\beta)$ remplira depuis 0 jusqu'à h les conditions exprimées dans l'énoncé (5). Les intégrales:

$$\int_0^g f(\beta) \frac{\sin i\beta}{\sin \beta} d\beta \quad \text{et} \quad \int_0^h f(\beta) \frac{\sin i\beta}{\sin \beta} d\beta$$

convergeront donc l'une et l'autre vers la limite $\frac{\pi}{2}f(0)$. D'où l'on conclut que l'intégrale $\int_g^h f(\beta) \frac{\sin i\beta}{\sin \beta} d\beta$, qui est la différence des précédentes, a zéro pour limite.

Ce nouveau résultat peut être réuni en un seul énoncé avec celui que nous avons obtenu plus haut. On aura ainsi:

$$(6) \left\{ \begin{array}{l} \text{La lettre } h \text{ désignant une quantité positive tout au plus égale à } \frac{\pi}{2}, \\ \text{et } g \text{ une quantité également positive et en outre inférieure à } h, \\ \text{l'intégrale:} \\ \int_g^h f(\beta) \frac{\sin i\beta}{\sin \beta} d\beta \\ \text{dans laquelle la fonction } f(\beta) \text{ est continue entre les limites de l'inté-} \\ \text{gration et a une marche toujours croissante ou toujours décroissante} \\ \text{depuis } \beta = g \text{ jusqu'à } \beta = h, \text{ convergera vers une certaine limite,} \\ \text{lorsque le nombre } i \text{ devient de plus en plus grand. Cette limite est} \\ \text{égale à zéro, le seul cas excepté où } g \text{ a une valeur nulle, dans ce} \\ \text{cas elle a la valeur } \frac{\pi}{2} f(0). \end{array} \right.$$

Il est évident que ce résultat ne serait que légèrement modifié, si la fonction $f(\beta)$ présentait une solution de continuité pour $\beta = g$ et $\beta = h$, c'est-à-dire si $f(g)$ était différent de $f(g+\varepsilon)$ et $f(h)$ de $f(h-\varepsilon)$, ε désignant une quantité infiniment petite et positive, pourvu qu'alors les valeurs $f(g)$ et $f(h)$ ne fussent pas infinies. Il faudrait seulement dans ce cas remplacer $f(0)$ par $f(\varepsilon)$ dans l'énoncé précédent, ce qu'on peut faire encore même quand il n'y a pas de solution de continuité, attendu qu'alors $f(\varepsilon)$ est égale à $f(0)$.

Nous sommes maintenant en état de prouver la convergence des séries périodiques qui expriment des fonctions arbitraires entre des limites données. La marche que nous allons suivre nous conduira à établir la convergence de ces séries et à déterminer en même temps leurs valeurs. Soit $g(x)$ une fonction de x , ayant une valeur finie et déterminée pour chaque valeur de x comprise entre $-\pi$ et π , et supposons qu'il s'agisse de développer cette fonction en une série de sinus et de cosinus d'arcs multiples de x . La série qui résout cette question, est, comme l'on sait:

$$(7) \quad \frac{1}{2\pi} \int g(\alpha) d\alpha + \frac{1}{\pi} \left\{ \begin{array}{l} \cos x \int g(\alpha) \cos \alpha d\alpha + \cos 2x \int g(\alpha) \cos 2\alpha d\alpha + \dots \\ \sin x \int g(\alpha) \sin \alpha d\alpha + \sin 2x \int g(\alpha) \sin 2\alpha d\alpha + \dots \end{array} \right\},$$

les intégrales qui déterminent les coefficients constants, étant prises depuis

$\alpha = -\pi$ jusqu'à $\alpha = \pi$, et x désignant une quantité quelconque comprise entre $-\pi$ et π (*Théorie de la Chaleur*, No. 232 et suiv.).

Considérons les $2n+1$ premiers termes de cette série (n étant un nombre entier) et voyons vers quelle limite converge la somme de ces termes, lorsque n devient de plus en plus grand. Cette somme peut être mise sous la forme suivante:

$$\frac{1}{\pi} \int_{-\pi}^{\pi} g(\alpha) d\alpha \left[\frac{1}{2} + \cos(\alpha-x) + \cos 2(\alpha-x) + \dots + \cos n(\alpha-x) \right].$$

ou en sommant la suite de cosinus:

$$(8) \quad \frac{1}{\pi} \int_{-\pi}^{\pi} g(\alpha) \frac{\sin(n+\frac{1}{2})(\alpha-x)}{2\sin\frac{1}{2}(\alpha-x)} d\alpha.$$

Tout se réduit maintenant à déterminer la limite dont cette intégrale approche sans cesse, lorsque n croît indéfiniment. Pour cela nous la partagerons en deux autres prises l'une depuis $-\pi$ jusqu'à x , l'autre depuis x jusqu'à π . Si l'on remplace dans la première α par $x-2\beta$, et dans la seconde α par $x+2\beta$, β étant une nouvelle variable, ces deux intégrales se changeront en celles-ci, abstraction faite du facteur $\frac{1}{\pi}$:

$$(9) \quad \int_0^{\frac{1}{2}(\pi+x)} \frac{\sin(2n+1)\beta}{\sin\beta} g(x-2\beta) d\beta \quad \text{et} \quad \int_0^{\frac{1}{2}(\pi-x)} \frac{\sin(2n+1)\beta}{\sin\beta} g(x+2\beta) d\beta.$$

Considérons la seconde de ces deux intégrales. La quantité x étant inférieure ou tout au plus égale à π , abstraction faite du signe, $\frac{1}{2}(\pi-x)$ ne pourra tomber hors des limites 0 et π . Si $\frac{1}{2}(\pi-x) = 0$, ce qui a lieu lorsque $x = \pi$, l'intégrale est nulle quel que soit n ; dans tous les autres cas elle convergera pour des valeurs croissantes de n vers une limite que nous allons déterminer. Supposons d'abord $\frac{1}{2}(\pi-x)$ inférieure ou tout au plus égale à $\frac{\pi}{2}$, et remarquons que la fonction $g(x+2\beta)$ peut présenter plusieurs solutions de continuité depuis $\beta = 0$ jusqu'à $\beta = \frac{1}{2}(\pi-x)$, et qu'elle peut aussi avoir plusieurs maxima et minima dans ce même intervalle. Désignons par $l, l', l'', \dots, l^{(v)}$, rangées selon l'ordre de leur grandeur, les différentes valeurs de β qui présentent l'une ou l'autre de ces circonstances, et décomposons notre intégrale en plusieurs autres prises respectivement entre les limites:

$$0 \text{ et } l, \quad l \text{ et } l', \quad l' \text{ et } l'', \quad \dots, \quad l^{(v)} \text{ et } \frac{1}{2}(\pi-x).$$

Toutes ces intégrales se trouveront dans le cas de l'énoncé (6). Elles convergeront donc toutes vers la limite zéro à mesure que n croît, à l'exception de la première qui converge vers la limite $\frac{\pi}{2} g(x+\epsilon)$, ϵ étant un nombre infiniment petit et positif. Si $\frac{1}{2}(\pi-x)$ était supérieure à $\frac{1}{2}\pi$, ce qui arrivera lorsque x a une valeur négative, on partagerait l'intégrale en deux autres, l'une prise depuis $\beta = 0$ jusqu'à $\beta = \frac{1}{2}\pi$, l'autre depuis $\beta = \frac{1}{2}\pi$ jusqu'à $\beta = \frac{1}{2}(\pi-x)$. La première de ces nouvelles intégrales se trouvera dans le même cas que celle que nous venons de considérer, elle convergera donc vers la limite $\frac{\pi}{2} g(x+\epsilon)$. Quant à la seconde, on peut la changer en celle-ci, en y remplaçant β par $\pi-\gamma$, γ étant une nouvelle variable:

$$\int_{\frac{1}{2}(\pi+x)}^{\frac{1}{2}\pi} g(x+2\pi-2\gamma) \frac{\sin(2n+1)(\pi-\gamma)}{\sin(\pi-\gamma)} d\gamma,$$

ou ce qui revient au même, n étant un entier:

$$\int_{\frac{1}{2}(\pi+x)}^{\frac{1}{2}\pi} g(x+2\pi-2\gamma) \frac{\sin(2n+1)\gamma}{\sin\gamma} d\gamma.$$

Elle a ainsi une forme analogue à celle de la précédente: en la décomposant comme précédemment en plusieurs autres, on verra qu'elle converge vers la limite zéro, le seul cas excepté, où $\frac{1}{2}(\pi+x)$ a une valeur nulle, c'est-à-dire lorsque $x = -\pi$; dans ce cas elle approche continuellement de la limite $g(\pi-\epsilon)$, ϵ ayant toujours la même signification. En résumant tout ce qui précède, on trouvera que la seconde des intégrales (9) est nulle lorsque $x = \pi$, qu'elle converge vers la limite $\frac{\pi}{2} [g(\pi-\epsilon) + g(-\pi+\epsilon)]$ lorsque $x = -\pi$, et que dans tous les autres cas elle approche continuellement de la limite $\frac{\pi}{2} g(x+\epsilon)$.

La première des intégrales (9) est entièrement analogue à la seconde; en y appliquant des considérations semblables, on trouvera qu'elle est nulle lorsque $x = -\pi$, qu'elle converge vers la limite $\frac{\pi}{2} [g(\pi-\epsilon) + g(-\pi+\epsilon)]$ lorsque $x = \pi$ et que dans tous les autres cas elle a pour limite $\frac{\pi}{2} g(x-\epsilon)$. Connaissant ainsi les limites de chacune des intégrales (9), il est facile de

trouver la limite dont l'intégrale (8) approche sans cesse, lorsque n devient de plus en plus grand; il suffit pour cela de se rappeler que cette intégrale est égale à la somme des intégrales (9) divisée par π . Or, l'intégrale (8) étant équivalente à la somme des $2n+1$ premiers termes de la série (7), il est prouvé que cette série est convergente, et l'on trouve au moyen des résultats précédents qu'elle est égale à :

$$\frac{1}{2}[g(x+\varepsilon)+g(x-\varepsilon)]$$

pour toute valeur de x comprise entre $-\pi$ et π , et que pour chacune des valeurs extrêmes π et $-\pi$, elle est égale à :

$$\frac{1}{2}[g(\pi-\varepsilon)+g(-\pi+\varepsilon)].$$

L'exposé précédent embrasse tous les cas: il se simplifie lorsque la valeur de x qu'on considère n'est pas une de celles qui présentent une solution de continuité. En effet les quantités $g(x+\varepsilon)$ et $g(x-\varepsilon)$ étant alors l'une et l'autre équivalentes à $g(x)$, on voit que la série a pour valeur $g(x)$.

Les considérations précédentes prouvent d'une manière rigoureuse que, si la fonction $g(x)$, dont toutes les valeurs sont supposées finies et déterminées, ne présente qu'un nombre fini de solutions de continuité entre les limites $-\pi$ et π , et si en outre elle n'a qu'un nombre déterminé de maxima et de minima entre ces mêmes limites, la série (7), dont les coefficients sont des intégrales définies dépendantes de la fonction $g(x)$, est convergente et a une valeur généralement exprimée par :

$$\frac{1}{2}[g(x+\varepsilon)+g(x-\varepsilon)],$$

où ε désigne un nombre infiniment petit. Il nous resterait à considérer les cas où les suppositions que nous avons faites sur le nombre des solutions de continuité et sur celui des valeurs maxima et minima cessent d'avoir lieu. Ces cas singuliers peuvent être ramenés à ceux que nous venons de considérer. Il faut seulement, pour que la série (8) présente un sens lorsque les solutions de continuité sont en nombre infini, que la fonction $g(x)$ remplisse la condition suivante.

Il est nécessaire qu'alors la fonction $g(x)$ soit telle que, si l'on désigne par a et b deux quantités quelconques comprises entre $-\pi$ et π , on puisse toujours placer entre a et b d'autres quantités r et s assez rapprochées pour que la fonction reste continue dans l'intervalle de r à s . On sentira

facilement la nécessité de cette restriction en considérant que les différents termes de la série sont des intégrales définies et en remontant à la notion fondamentale des intégrales. On verra alors que l'intégrale d'une fonction ne signifie quelque chose qu'autant que la fonction satisfait à la condition précédemment énoncée. On aurait un exemple d'une fonction qui ne remplit pas cette condition, si l'on supposait $g(x)$ égale à une constante déterminée c lorsque la variable x obtient une valeur rationnelle, et égale à une autre constante d , lorsque cette variable est irrationnelle. La fonction ainsi définie a des valeurs finies et déterminées pour toute valeur de x , et cependant on ne saurait la substituer dans la série, attendu que les différentes intégrales qui entrent dans cette série, perdraient toute signification dans ce cas. La restriction que je viens de préciser, et celle de ne pas devenir infinie, sont les seules auxquelles la fonction $g(x)$ soit sujette et tous les cas qu'elles n'excluent pas peuvent être ramenés à ceux que nous avons considérés dans ce qui précède. Mais la chose, pour être faite avec toute la clarté qu'on peut désirer, exige quelques détails liés aux principes fondamentaux de l'analyse infinitésimale et qui seront exposés dans une autre note, où je m'occuperai aussi de quelques autres propriétés assez remarquables de la série (7).

Berlin, Janvier 1829.

ÜBER DIE DARSTELLUNG GANZ WILLKÜR-
LICHER FUNCTIONEN DURCH SINUS- UND
COSINUSREIHEN.

VON

G. LEJEUNE DIRICHLET.

Repertorium der Physik, unter Mitwirkung der Herren Lejeune Dirichlet, Jacobi, Neumann,
Riess, Strehlke, herausgegeben von Heinrich Wilhelm Dove und Ludwig Moser.
Bd. I, 1837, S. 152—174.

ÜBER DIE DARSTELLUNG GANZ WILLKÜRLICHER FUNCTIONEN DURCH SINUS- UND COSINUSREIHEN.

Die merkwürdigen Reihen, welche in einem bestimmten Intervalle Functionen darstellen, welche ganz gesetzlos sind oder in verschiedenen Theilen dieses Intervalls ganz verschiedenen Gesetzen folgen, haben seit der Begründung der mathematischen Wärmelehre durch FOURIER so zahlreiche Anwendungen in der analytischen Behandlung physikalischer Probleme gefunden, dass es zweckmässig erscheint, die für die folgenden Bände dieses Werkes bestimmten Auszüge aus den neuesten Arbeiten über einige Theile der mathematischen Physik durch die Entwicklung einiger der wichtigsten dieser Reihen einzuleiten.

§. 1.

Man denke sich unter a und b zwei feste Werthe und unter x eine veränderliche Grösse, welche nach und nach alle zwischen a und b liegenden Werthe annehmen soll. Entspricht nun jedem x ein einziges, endliches y , und zwar so, dass, während x das Intervall von a bis b stetig durchläuft, $y = f(x)$ sich ebenfalls allmählich verändert, so heisst y eine stetige oder continuirliche*) Function von x für dieses Intervall. Es ist dabei gar nicht nöthig, dass y in diesem ganzen Intervalle nach demselben Gesetze von x abhängig sei, ja man braucht nicht einmal an eine durch mathematische Operationen ausdrückbare Abhängigkeit zu denken. Geometrisch dargestellt, d. h. x und y als Abscisse und Ordinate gedacht, erscheint eine stetige Function als eine zusammenhängende Curve, von der jeder zwischen a und b enthaltenen Abscisse nur ein Punkt entspricht. Diese Definition schreibt den einzelnen Theilen der Curve kein gemeinsames Gesetz vor; man kann sich dieselbe aus den verschiedenartigsten Theilen zusammengesetzt oder ganz gesetzlos gezeichnet denken. Es

*) Da im Folgenden nur von stetigen Functionen die Rede sein wird, so kann der Zusatz ohne Nachtheil wegbleiben.

geht hieraus hervor, dass eine solche Function für ein Intervall als vollständig bestimmt nur dann anzusehen ist, wenn sie entweder für den ganzen Umfang desselben graphisch gegeben ist, oder mathematischen, für die einzelnen Theile desselben geltenden Gesetzen unterworfen wird. So lange man über eine Function nur für einen Theil des Intervalls bestimmt hat, bleibt die Art ihrer Fortsetzung für das übrige Intervall ganz der Willkür überlassen.

Es seien A und B die Endpunkte von a und b , und $\alpha\gamma\beta$ die der Function $f(x)$ entsprechende Curve, so ist klar, dass mit dieser Function auch der Flächenraum $A\alpha\gamma\beta B$ bestimmt ist, welcher von den Ordinaten $A\alpha$, $B\beta$, dem Stück AB der Abscissenachse und der Curve $\alpha\gamma\beta$ begrenzt wird, wenn er sich gleich nicht immer genau angeben lässt. Dieser Raum heisst bekanntlich auch das bestimmte Integral der Function $f(x)$, von a bis b oder zwischen den Grenzen a und b genommen, und wird durch $\int_a^b f(x) dx$ bezeichnet. Der Ursprung dieses Zeichens liegt in der Art, wie die Infinitesimalrechnung einen Flächenraum oder ein solches Integral betrachtet. Wird die Linie $AB = b - a$, in eine Anzahl n gleicher Theile zerlegt, deren gemeinschaftlicher Werth $= \frac{b-a}{n} = \delta$, und werden durch α und die Endpunkte der den Theilungspunkten 1, 2, 3, ... entsprechenden Ordinaten, Parallelen mit der Abscissenachse gezogen, so entstehen n Rechtecke, deren Summe:

$$(1) \quad \delta f(a) + \delta f(a + \delta) + \delta f(a + 2\delta) + \dots + \delta f(a + (n-1)\delta),$$

wie sich leicht streng beweisen lässt, und wie es auch schon die blosser Anschauung ergibt, bei unaufhörlichem Wachsen der Anzahl n zuletzt in den Flächenraum $A\alpha\gamma\beta B$ übergeht, d. h. man kann n immer so gross wählen, dass die Summe (1) von diesem Raum um weniger verschieden sein wird, als eine noch so kleine, vorher bestimmte Grösse. Nimmt man $b - a$ und also auch δ als positiv an, so erscheinen offenbar die in (1) enthaltenen Rechtecke als positiv oder negativ, je nachdem sie auf der Seite der positiven oder der negativen y liegen. Umgekehrt verhält es sich, wenn $b - a$ negativ ist. Es geht also hieraus hervor, dass ein bestimmtes Integral $\int_a^b f(x) dx$ (wenn man dieses als den Grenzwert betrachtet, welchen (1) für ein unendliches n annimmt) nur insofern als Flächenraum angesehen werden kann, als man bei letzterem die Theile, welche auf entgegengesetzten Seiten der Abscissenachse liegen, ent-

gegengesetzt und zwar die auf der Seite der positiven y liegenden als positiv oder negativ nimmt, je nachdem b grösser oder kleiner als a ist.

§. 2.

Aus der Definition des bestimmten Integrals als Grenzwert von (1) oder als Flächenraum mit der eben angegebenen Modification folgen fast unmittelbar mehrere Eigenschaften, die ich hier zusammenstelle, um mich im Folgenden leichter darauf berufen zu können: c bezeichnet, wie a und b , eine Constante.

$$(2) \quad \int_a^b j(x) dx = - \int_b^a j(x) dx,$$

$$(3) \quad \int_a^b c j(x) dx = c \int_a^b j(x) dx,$$

$$(4) \quad \int_a^b j(x) dx = \int_{a+c}^{b+c} j(x-c) dx,$$

$$(5) \quad \int_a^b j(x) dx = \frac{1}{c} \int_{ac}^{bc} j\left(\frac{x}{c}\right) dx,$$

$$(6) \quad \int_a^b [j(x) \pm F(x)] dx = \int_a^b j(x) dx \pm \int_a^b F(x) dx,$$

(7) $\left\{ \begin{array}{l} \text{Hat } j(x) \text{ zwischen } x = a \text{ und } x = b \text{ immer dasselbe Zeichen, so ist} \\ \int_a^b j(x) dx \text{ positiv oder negativ, je nachdem jenes Zeichen dem von } b - a \\ \text{gleich oder entgegengesetzt ist.} \end{array} \right.$

(8) $\left\{ \begin{array}{l} \text{Das Integral } \int_a^b \varphi(x) F(x) dx \text{ liegt immer zwischen } M \int_a^b F(x) dx \text{ und} \\ N \int_a^b F(x) dx, \text{ wenn } F(x) \text{ innerhalb der Grenzen } a \text{ und } b \text{ sein Zeichen} \\ \text{nicht ändert und } M \text{ und } N \text{ respective den grössten und kleinsten} \\ \text{Werth*) bezeichnen, den } \varphi(x) \text{ in dem genannten Intervall erhält.} \end{array} \right.$

Dieser Satz, welcher im Folgenden häufig Anwendung findet, ist leicht aus den vorhergehenden abzuleiten. Nach den über M und N gemachten Vor-

*) Es ist wohl zu bemerken, dass hier bei der Vergleichung zweier Werthe hinsichtlich ihrer Grösse auf die Zeichen Rücksicht genommen wird; r heisst grösser als s , oder geschrieben: $r > s$, wenn die algebraische Differenz $r - s$ positiv ist.

aussetzungen bleiben:

$$M - g(x), \quad g(x) - N$$

zwischen $x = a$ und $x = b$ stets positiv:

$$[M - g(x)]F(x), \quad [g(x) - N]F(x)$$

sind daher in diesem Intervall entweder beide immer positiv oder beide immer negativ, woraus vermöge (7) folgt, dass die Integrale:

$$\int_a^b [M - g(x)]F(x)dx, \quad \int_a^b [g(x) - N]F(x)dx$$

gleiche Zeichen haben. Werden diese Integrale nach (6) und (3) in die Form:

$$M \int_a^b F(x)dx - \int_a^b g(x)F(x)dx, \quad \int_a^b g(x)F(x)dx - N \int_a^b F(x)dx$$

gebracht, so ist die Behauptung bewiesen.

$$(9) \quad \left\{ \begin{array}{l} \text{Liegt } c \text{ zwischen } a \text{ und } b, \text{ so ist:} \\ \int_a^b f(x)dx = \int_a^c f(x)dx + \int_c^b f(x)dx. \end{array} \right.$$

Dieser Satz sagt nichts anderes, als dass der Flächenraum $\int_a^b f(x)dx$ durch die der Abscisse c entsprechende Ordinate in zwei andere Flächenräume zerlegt wird. Man kann durch wiederholte Anwendung desselben jedes Integral in eine beliebige Anzahl anderer Integrale zerlegen.

Es geht z. B. daraus hervor,

$$(10) \quad \left\{ \begin{array}{l} \text{dass } \int_0^\pi \cos 2m x dx = 0, \text{ wenn } m \text{ irgend eine von } 0 \text{ verschiedene ganze} \\ \text{Zahl bezeichnet.} \end{array} \right.$$

Zerlegt man nämlich diesen Flächenraum in $2m$ andere zwischen den Grenzen:

$$0 \text{ und } \frac{\pi}{4m}, \quad \frac{\pi}{4m} \text{ und } \frac{2\pi}{4m}, \quad \frac{2\pi}{4m} \text{ und } \frac{3\pi}{4m}, \quad \dots, \quad \frac{(2m-1)\pi}{4m} \text{ und } \frac{2m\pi}{4m},$$

so sieht man leicht, dass der erste dem zweiten, der dritte dem vierten u. s. w. gleich und entgegengesetzt ist.

Endlich ist für das Folgende noch die Kenntniss der Summe z der endlichen Reihe:

$$z = \cos \vartheta + \cos 2\vartheta + \dots + \cos n\vartheta$$

erforderlich. Um zur Bestimmung derselben zu gelangen, multiplicire man die

Gleichung mit $2\cos\vartheta$ und verwandle die Cosinusproducte nach der bekannten Formel $2\cos\beta\cos\gamma = \cos(\beta-\gamma) + \cos(\beta+\gamma)$ in Summen. Man erhält so:

$$2z\cos\vartheta = 1 + \cos\vartheta + \cos 2\vartheta + \dots + \cos(n-1)\vartheta \\ + \cos 2\vartheta + \cos 3\vartheta + \cos 4\vartheta + \dots + \cos(n+1)\vartheta.$$

Die Vergleichung der oberen Horizontalreihe mit der durch z bezeichneten Reihe ergibt für dieselbe:

$$z + 1 - \cos n\vartheta;$$

eben so findet man für die untere:

$$z - \cos\vartheta + \cos(n+1)\vartheta.$$

Werden beide Werthe eingesetzt, so kommt:

$$2z\cos\vartheta = 2z + 1 - \cos\vartheta + \cos(n+1)\vartheta - \cos n\vartheta;$$

Bringt man $2z$ auf die andere Seite und dividirt durch $2(\cos\vartheta - 1)$, so folgt:

$$z = -\frac{1}{2} + \frac{\cos n\vartheta - \cos(n+1)\vartheta}{2(1 - \cos\vartheta)}.$$

Dieser Ausdruck für z wird vereinfacht, wenn man $2\sin^2\frac{1}{2}\vartheta$ für $1 - \cos\vartheta$ und $2\sin\frac{1}{2}\vartheta\sin(n+\frac{1}{2})\vartheta$ für $\cos n\vartheta - \cos(n+1)\vartheta$ einführt und den gemeinschaftlichen Factor $2\sin\frac{1}{2}\vartheta$ weglässt. Man findet so:

$$(11) \quad \cos\vartheta + \cos 2\vartheta + \dots + \cos n\vartheta = -\frac{1}{2} + \frac{\sin(n+\frac{1}{2})\vartheta}{2\sin\frac{1}{2}\vartheta}.$$

§. 3.

Verschiedene Aufgaben der mathematischen Physik erfordern die Darstellung einer für das Intervall von 0 bis π ganz willkürlich gegebenen Function $f(x)$ durch eine unendliche Reihe von folgender Form:

$$a_1 \sin x + a_2 \sin 2x + a_3 \sin 3x + \dots,$$

wo a_1, a_2, a_3, \dots von x unabhängige Grössen bezeichnen. Der natürlichste Weg zu der verlangten Reihenentwicklung scheint der sogenannte Uebergang vom Endlichen zum Unendlichen zu sein. Man denke sich nämlich zunächst die Reihe aus einer endlichen Anzahl $(n-1)$ von Gliedern bestehend, d. h. man betrachte den Ausdruck:

$$a_1 \sin x + a_2 \sin 2x + \dots + a_{n-1} \sin(n-1)x.$$

Die darin enthaltenen willkürlichen $n-1$ Coefficienten a_1, a_2, \dots, a_{n-1} lassen sich so bestimmen, dass dieser Ausdruck für eben so viele besondere Werthe von x , nämlich $\frac{\pi}{n}, \frac{2\pi}{n}, \dots, (n-1)\frac{\pi}{n}$, der gegebenen Function $f(x)$

Jede dieser Reihen lässt sich nach Formel (11) summiren. Wenn man dort $\vartheta = (m-h)\frac{\pi}{n}$ setzt und n in $n-1$ verwandelt, so findet man für die erste:

$$-\frac{1}{2} + \frac{\sin(n-\frac{1}{2})(m-h)\frac{\pi}{n}}{2\sin(m-h)\frac{\pi}{2n}}.$$

Erinnert man sich, dass für irgend eine ganze Zahl l :

$$\sin(l\pi - \gamma) = \mp \sin \gamma,$$

wo das obere oder das untere Zeichen gilt, je nachdem l gerade oder ungerade ist, so sieht man gleich, dass:

$$\sin(n-\frac{1}{2})(m-h)\frac{\pi}{n} = \sin\left((m-h)\pi - (m-h)\frac{\pi}{2n}\right) = \mp \sin(m-h)\frac{\pi}{2n},$$

und dass also die erste der Reihen (12):

$$\cos(m-h)\frac{\pi}{n} + \cos 2(m-h)\frac{\pi}{n} + \dots + \cos(n-1)(m-h)\frac{\pi}{n}$$

den Werth -1 oder 0 hat, je nachdem $m-h$ gerade oder ungerade ist. Aehnlicherweise ergibt sich für die zweite Reihe (12):

$$-\left(\cos(m+h)\frac{\pi}{n} + \cos 2(m+h)\frac{\pi}{n} + \dots + \cos(n-1)(m+h)\frac{\pi}{n}\right)$$

den Werth $+1$ oder 0 , je nachdem $m+h$ gerade oder ungerade ist. Bemerket man nun, dass $m-h$ und $m+h$ entweder zugleich gerade oder zugleich ungerade sind, da ihre Summe $2m$ gerade ist, so sieht man auf der Stelle, dass der Ausdruck (12) verschwindet, wie es früher behauptet wurde.

Es ist nicht zu übersehen, dass das oben gefundene Resultat wesentlich voraussetzt, dass h von m verschieden ist. Für den Fall, wo $h = m$, erscheint der Ausdruck für die Summe der ersten der Reihen (12) in der Form $\frac{0}{0}$, und die vorige Bestimmung verliert ihre Gültigkeit. Man erhält aber in diesem Falle, da alle Glieder dieser Reihe der Einheit gleich werden, sogleich für ihre Summe $n-1$, während die zweite den Werth 1 annimmt, indem $m+h = 2m$ in diesem Falle gerade ist. Der Ausdruck (12) verschwindet also für jedes h , welches von m verschieden ist, für $h = m$ hingegen erhält er den Werth n . Es geht daraus hervor, dass die Gleichung, deren Entstehung man oben näher angegeben hat, in der That nur den einzigen Coefficienten a_m enthält und von folgender sehr einfachen Form ist:

$$na_m = 2\sin\frac{m\pi}{n} f\left(\frac{\pi}{n}\right) + 2\sin\frac{2m\pi}{n} f\left(\frac{2\pi}{n}\right) + \dots + 2\sin(n-1)\frac{m\pi}{n} f\left(\frac{(n-1)\pi}{n}\right)$$

und folglich:

$$a_m = \frac{2}{n} \left[\sin \frac{m\pi}{n} f\left(\frac{\pi}{n}\right) + \sin \frac{2m\pi}{n} f\left(\frac{2\pi}{n}\right) + \dots + \sin(n-1) \frac{m\pi}{n} f\left(\frac{(n-1)\pi}{n}\right) \right].$$

Nachdem die Coefficienten der endlichen Reihe gefunden worden sind, bleibt zu untersuchen, wie sich der Coefficient, welcher eine beliebige, aber bestimmte Stelle einnimmt, bei unaufhörlich wachsender Gliederzahl verändert, d. h. es bleibt der Werth auszumitteln, den der vorhergehende Ausdruck für a_m annimmt, wenn man n unendlich gross werden lässt, während m constant gedacht wird. Schreibt man den Ausdruck wie folgt:

$$a_m = \frac{2}{\pi} \left[\frac{\pi}{n} \sin\left(\frac{0m\pi}{n}\right) f\left(\frac{0\pi}{n}\right) + \frac{\pi}{n} \sin\left(\frac{m\pi}{n}\right) f\left(\frac{\pi}{n}\right) + \frac{\pi}{n} \sin\left(\frac{2m\pi}{n}\right) f\left(\frac{2\pi}{n}\right) + \dots \right. \\ \left. \dots + \frac{\pi}{n} \sin(n-1) \frac{m\pi}{n} f\left(\frac{(n-1)\pi}{n}\right) \right].$$

so erhellt sogleich aus der Vergleichung der Summe zwischen den Klammern mit der Gleichung (1), dass für $n = \infty$ die Summe in das bestimmte Integral $\int_0^\pi \sin mx f(x) dx$ übergeht.

Die alsdann zu einer unendlichen gewordene Reihe stellt aber, wie früher bemerkt worden, die Function $f(x)$ für alle zwischen 0 und π gelegenen Werthe von x dar, und wir haben also für den ganzen Umfang des genannten Intervalls:

$$(13) \quad f(x) = a_1 \sin x + a_2 \sin 2x + \dots + a_m \sin mx + \dots,$$

in welcher Reihe die Coefficienten nach der allgemeinen Gleichung:

$$a_m = \frac{2}{\pi} \int_0^\pi \sin mx f(x) dx$$

zu bestimmen sind.

Man kann durch ähnliche Betrachtungen zu einer Reihe gelangen, welche nur die Cosinus von x und dessen Vielfachen enthält, und die Function $f(x)$, wie die gefundene Sinusreihe, für dasselbe Intervall von 0 bis π darstellt. Kürzer erreicht man jedoch diesen Zweck, wenn man das schon gefundene Resultat (13) benutzt. Setzt man in demselben statt $f(x)$ das Product $2f(x)\sin x$, so erhält man:

$$2\sin x f(x) = a_1 \sin x + a_2 \sin 2x + \dots + a_m \sin mx + \dots,$$

wo:

$$a_m = \frac{2}{\pi} \int_0^\pi 2\sin mx \sin x f(x) dx.$$

Dieser Werth für a_m lässt sich auch so schreiben:

$$a_m = \frac{2}{\pi} \int_0^\pi \cos(m-1)x f(x) dx - \frac{2}{\pi} \int_0^\pi \cos(m+1)x f(x) dx,$$

oder, wenn man zur Abkürzung setzt:

$$\frac{2}{\pi} \int_0^\pi \cos hx f(x) dx = b_h,$$

wo h eine ganze positive Zahl mit Einschluss der Null bezeichnet:

$$a_m = b_{m-1} - b_{m+1}.$$

Nimmt man successive $m = 1, 2, 3, \dots$ und substituirt in obige Reihe, so kommt:

$$2\sin x f(x) = (b_0 - b_2)\sin x + (b_1 - b_3)\sin 2x + (b_2 - b_4)\sin 3x + \dots,$$

oder wenn man nach b_0, b_1, b_2, \dots ordnet:

$$2\sin x f(x) = b_0 \sin x + b_1 \sin 2x + b_2 (\sin 3x - \sin x) + b_3 (\sin 4x - \sin 2x) + \text{etc.}$$

Durch Einführung der Producte $2\sin x \cos x, 2\sin x \cos 2x, \dots$ an die Stelle von $\sin 2x, \sin 3x - \sin x, \dots$ wird die ganze Gleichung durch $2\sin x$ theilbar, und man erhält nach Entfernung dieses gemeinschaftlichen Factors:

$$(14) \quad f(x) = \frac{1}{2} b_0 + b_1 \cos x + b_2 \cos 2x + \dots + b_m \cos mx + \dots$$

Diese Gleichung gilt wie die Gleichung (13), aus der sie abgeleitet ist, für alle Werthe zwischen 0 und π , und der allgemeine Coefficient b_m ist:

$$\frac{2}{\pi} \int_0^\pi \cos mx f(x) dx.$$

Obgleich die Reihen (13) und (14) beide eine ganz beliebige Function $f(x)$ für das Intervall von 0 bis π darstellen, so sind sie doch wesentlich von einander verschieden. Während die letztere wegen der bekannten Eigenschaft des Cosinus, für entgegengesetzte Werthe des Bogens gleich zu sein, durch die Verwandlung von x in $-x$ unverändert bleibt, nimmt die erstere in demselben Falle den entgegengesetzten Werth an, wie eben so leicht aus der Natur des Sinus erhellt. Man sieht hieraus leicht, dass man unter gewissen Umständen eine Function von x für das Intervall von $-\pi$ bis π durch die Reihe (14) oder (13) darstellen kann. Denkt man sich nämlich unter $f(x)$ eine von $x = 0$ bis $x = \pi$ ganz beliebig gegebene Function von x , und setzt diese Function oder Curve von $x = 0$ bis $x = -\pi$ so fort, dass immer:

$$f(-x) = f(x),$$

so wird diese Function von $x = \pi$ bis $x = -\pi$, durch die Reihe (14) ausgedrückt werden können, denn diese Reihe gilt immer von 0 bis π , und da sie bei der Verwandlung von x in $-x$ unverändert bleibt, welches nach der angegebenen Art der Fortsetzung auch bei der Function der Fall ist, so stellt sie diese auch von 0 bis $-\pi$ dar. Ganz auf dieselbe Weise überzeugt man sich, dass wenn man eine von 0 bis π beliebig gegebene Function so fortsetzt, dass:

$$f(-x) = -f(x).$$

für eine solche Function zwischen $x = -\pi$ und $x = \pi$ die Reihe (13) gilt. Auf diese einfache Bemerkung kann man eine Reihe gründen, welche die Reihen (13) und (14) als besondere Fälle in sich begreift und eine von $x = -\pi$ bis $x = \pi$ ganz willkürlich gegebene Function $g(x)$ darzustellen geeignet ist. — Bringt man nämlich $g(x)$ in die Form:

$$\frac{g(x)+g(-x)}{2} + \frac{g(x)-g(-x)}{2},$$

so hat der erste Theil $\frac{g(x)+g(-x)}{2}$ die Eigenschaft, durch Verwandlung von x in $-x$ unverändert zu bleiben, und ist also nach dem Vorhergehenden von $x = -\pi$ bis $x = \pi$ durch (14) ausdrückbar. Eben so lässt sich offenbar der zweite Theil $\frac{g(x)-g(-x)}{2}$ durch die Reihe (13) darstellen, und man hat also für den ganzen Umfang des Intervalls von $-\pi$ bis π , wenn man beide Theile vereinigt:

$$(15) \quad \left\{ \begin{aligned} g(x) &= \frac{1}{2} b_0 + b_1 \cos x + b_2 \cos 2x + \dots + b_m \cos mx + \dots \\ &\quad + a_1 \sin x + a_2 \sin 2x + \dots + a_m \sin mx + \dots, \end{aligned} \right.$$

wo die Coefficienten durch die Gleichungen:

$$b_m = \frac{1}{\pi} \int_0^\pi \cos mx [g(x) + g(-x)] dx,$$

$$a_m = \frac{1}{\pi} \int_0^\pi \sin mx [g(x) - g(-x)] dx$$

zu bestimmen sind. Man kann diesen Ausdrücken eine einfachere Form geben. Es ist nämlich:

$$\int_0^\pi \cos mx [g(x) + g(-x)] dx = \int_0^\pi \cos mx g(x) dx + \int_0^\pi \cos mx g(-x) dx$$

und nach (5):

$$\int_0^\pi \cos mx g(-x) dx = - \int_0^{-\pi} \cos mx g(x) dx,$$

oder nach (2), $= \int_{-\pi}^0 \cos mx \mathbf{q}(x) dx$, folglich:

$$b_m = \frac{1}{\pi} \left(\int_{-\pi}^0 \cos mx \mathbf{q}(x) dx + \int_0^{\pi} \cos mx \mathbf{q}(x) dx \right)$$

oder nach (9):

$$b_m = \frac{1}{\pi} \int_{-\pi}^{+\pi} \cos mx \mathbf{q}(x) dx.$$

Ebenso ergibt sich:

$$a_m = \frac{1}{\pi} \int_{-\pi}^{+\pi} \sin mx \mathbf{q}(x) dx.$$

§. 4.

Wie natürlich und wie befriedigend auch auf den ersten Blick der Gang erscheinen mag, welcher uns zu den Reihen des vorigen Paragraphen geführt hat, so findet man doch bald bei genauerer Erwägung, dass derselbe als strenger Beweis für die Gültigkeit dieser Reihen etwas zu wünschen übrig lässt. Es geht aus dem Begriff des bestimmten Integrals, wie dieser in (1) festgestellt wurde, unbestreitbar hervor, dass irgend ein Coefficient a_m , welcher in der endlichen Reihe eine bestimmte Stelle m einnimmt, bei unaufhörlichem Wachsen von n in das Integral $\frac{2}{\pi} \int_0^{\pi} \sin mx f(x) dx$ übergeht, allein man darf nicht vergessen,

dass durch das Zunehmen von n zugleich immer mehr neue Glieder hinzukommen. Um die Richtigkeit der Reihe (13) zu beweisen, müsste man sich die Glieder der endlichen Reihe in zwei Gruppen zerfällt denken: die erste würde alle Glieder bis zu einer bestimmten unveränderlich gedachten Stellenzahl m , die zweite alle übrigen enthalten. Könnte man nun zeigen, dass, während die Coefficienten der Glieder der ersten Gruppe sich ins Unendliche den durch bestimmte Integrale ausgedrückten Werthen nähern, der Inbegriff aller Glieder der zweiten, deren Anzahl mit n unaufhörlich wächst, nie eine gewisse von m abhängige und zwar beliebig klein ausfallende Grenze überschreitet, wenn man das m gehörig gross wählte, so würde man die Gewissheit erlangen, dass die Reihe (13) convergirend ist und die Function $f(x)$ für das Intervall von 0 bis π wirklich darstellt. — Die Nothwendigkeit der eben angedeuteten Nachweisung, wenn man den Uebergang vom Endlichen zum Unendlichen zu einem ganz strengen Verfahren erheben will, wird im höchsten

Grade einleuchtend, wenn man der endlichen Reihe, von der man ausgeht, eine andere Form giebt. Betrachtet man eine Reihe von der Form:

$$a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1},$$

so lassen sich die Coefficienten ebenfalls leicht so bestimmen, dass die Reihe für n Werthe von x innerhalb eines beliebigen Intervalls einer ganz willkürlichen Function $f(x)$ gleich wird. Lässt man nach erlangter Bestimmung irgend eines Coefficienten n unendlich wachsen, während die Stellenzahl m der Coefficienten constant bleibt, so nähert sich der Coefficient unaufhörlich einem gewissen Endwerth, und man würde also durch das im vorigen Paragraphen befolgte Verfahren zu der falschen Folgerung verleitet, eine ganz gesetzlose oder stellenweise ganz anderen Gesetzen gehorchende Function lasse sich durch eine nach Potenzen der Veränderlichen x geordnete Reihe darstellen.

Die Betrachtungen, die dem Verfahren, welches uns die Reihe (13) geliefert hat, die gehörige Strenge geben würden, sind so zusammengesetzter Art, dass wir lieber einen andern Weg der Beweisführung einschlagen. Wir werden die Reihe (15), welche die beiden andern (13) und (14) als besondere Fälle in sich begreift, an und für sich untersuchen und, ohne etwas von dem Früheren voranzusetzen, direct nachweisen, dass diese Reihe:

$$\frac{1}{2}b_0 + b_1 \cos x + b_2 \cos 2x + \dots + b_m \cos mx + \dots \\ + a_1 \sin x + a_2 \sin 2x + \dots + a_m \sin mx + \dots,$$

wenn man ihre Coefficienten durch die Gleichungen:

$$b_m = \frac{1}{\pi} \int_{-\pi}^{+\pi} \cos mxy(x) dx, \quad a_m = \frac{1}{\pi} \int_{-\pi}^{+\pi} \sin mxy(x) dx$$

bestimmt, immer convergirt und für alle zwischen $-\pi$ und π enthaltenen Werthe von x der Function $g(x)$ gleich ist.

Schreibt man in den vorhergehenden Integralen statt x einen andern Buchstaben u , was offenbar erlaubt ist, da ein bestimmtes Integral nur von der Natur der Function und den Werthen der Grenzen abhängig ist, und setzt die Werthe für die $2n+1$ ersten Coefficienten ein, so erhält man als Summe der $2n+1$ ersten Glieder der Reihe:

$$\frac{1}{2\pi} \int_{-\pi}^{+\pi} du g(u) + \frac{1}{\pi} \cos x \int_{-\pi}^{+\pi} du \cos u g(u) + \dots + \frac{1}{\pi} \cos nx \int_{-\pi}^{+\pi} du \cos nu g(u) \\ + \frac{1}{\pi} \sin x \int_{-\pi}^{+\pi} du \sin u g(u) + \dots + \frac{1}{\pi} \sin nx \int_{-\pi}^{+\pi} du \sin nu g(u)$$

oder nach (3) und (6):

$$\frac{1}{\pi} \int_{-\pi}^{+\pi} du g(u) [\frac{1}{2} + \cos(u-x) + \cos 2(u-x) + \dots + \cos n(u-x)]$$

oder endlich, wenn man die Cosinusreihe vermittelt der Formel (11) summiert:

$$\frac{1}{\pi} \int_{-\pi}^{+\pi} du g(u) \frac{\sin(2n+1) \frac{u-x}{2}}{2 \sin \frac{u-x}{2}}.$$

Soll also die Reihe convergiren und den Werth $g(x)$ haben, so muss der Unterschied zwischen $g(x)$ und diesem Integral, welches die Summe ihrer $2n+1$ ersten Glieder ausdrückt, bei manföhrlichem Zunehmen von n zuletzt kleiner werden als jede noch so klein gedachte Grösse. Es ist nöthig, der Untersuchung dieses Integrals in seiner ganzen Allgemeinheit die Behandlung einiger einfachen Fälle voranzuschicken, auf welche sich alle übrigen zurückführen lassen.

§. 5.

Man betrachte zunächst das Integral:

$$\int_0^{\pi} \frac{\sin(2n+1)\beta}{\sin \beta} d\beta,$$

in welchem n wie vorher eine positive ganze Zahl bezeichnet. Setzt man statt $\frac{\sin(2n+1)\beta}{\sin \beta}$ den nach (11) äquivalenten Ausdruck:

$$1 + 2\cos 2\beta + 2\cos 4\beta + \dots + 2\cos 2n\beta,$$

so erhellt nach (10), dass alle Glieder mit Ausnahme des ersten zwischen den angegebenen Grenzen integrirt verschwinden, und man findet:

$$\int_0^{\pi} \frac{\sin(2n+1)\beta}{\sin \beta} d\beta = \frac{\pi}{2}.$$

Setzt man zur Abkürzung $2n+1 = k$ und zerlegt das Integral in $n+1$ andere zwischen den Grenzen 0 und $\frac{\pi}{k}$, $\frac{\pi}{k}$ und $\frac{2\pi}{k}$, \dots , $\frac{n\pi}{k}$ und $\frac{\pi}{2}$, so folgt nach (7), dass von diesen Integralen das erste positiv, das zweite negativ, das dritte positiv u. s. w. sein wird, da $\frac{\sin k\beta}{\sin \beta}$ innerhalb der Grenzen des ersten positiv, des zweiten negativ u. s. w. ist. Bezeichnet man das Integral des Ranges ν ,

d. h. das von $\frac{(v-1)\pi}{k}$ bis $\frac{v\pi}{k}$ genommene, abgesehen von seinem Zeichen, mit q_v , so dass also:

$$q_v = \mp \int_{\frac{(v-1)\pi}{k}}^{\frac{v\pi}{k}} \frac{\sin k\beta^2}{\sin \beta} d\beta.$$

wo das obere oder untere Zeichen gilt, je nachdem v gerade oder ungerade ist, so folgt leicht aus (8), da $\mp \sin k\beta^2$ von $\frac{(v-1)\pi}{k}$ bis $\frac{v\pi}{k}$ stets positiv bleibt, dass q_v zwischen den beiden Producten liegt, welche man erhält, wenn man:

$$\int_{\frac{(v-1)\pi}{k}}^{\frac{v\pi}{k}} \mp \sin k\beta^2 d\beta = \frac{2}{k}$$

mit dem grössten und kleinsten Werth multiplicirt, den der Factor $\frac{1}{\sin \beta}$ in dem genannten Intervall annimmt.

Das vorhergehende Integral ist nach (4):

$$= \int_0^{\pi} \mp \sin((v-1)\pi + k\beta) d\beta = \int_0^{\pi} \sin k\beta d\beta.$$

oder nach (5):

$$= \frac{1}{k} \int_0^{\pi} \sin \beta d\beta = \frac{A}{k}.$$

wenn man zur Abkürzung den von k unabhängigen Werth $\int_0^{\pi} \sin \beta d\beta$ mit A bezeichnet.

Was den Factor $\frac{1}{\sin \beta}$ betrifft, so ist dieser um so kleiner, als β grösser ist. Sein grösster Werth ist daher $\frac{1}{\sin \frac{(v-1)\pi}{k}}$ und der kleinste $\frac{1}{\sin \frac{v\pi}{k}}$, so

dass also:

$$q_v > \frac{A}{k} \frac{1}{\sin \frac{v\pi}{k}} \quad \text{und} \quad q_v < \frac{A}{k} \frac{1}{\sin \frac{(v-1)\pi}{k}}.$$

Für das letzte Integral q_{n+1} gelten die Grenzen $\frac{A}{k}$ und $\frac{A}{k} \frac{1}{\sin \frac{1}{n\pi}}$, die sich auf dieselbe Weise ergeben. Vergleicht man die Grenzen, zwischen welchen

je zwei auf einander folgende Integrale liegen, so ergibt sich auf der Stelle, dass $q_1, q_2, q_3, \dots, q_{n+1}$ eine abnehmende Reihe bilden, d. h.:

$$q_1 > q_2 > q_3 > \dots > q_{n+1}.$$

Das ursprüngliche, später in $n+1$ andre Integrale zerlegte Integral hatte den Werth $\frac{\pi}{2}$. Es findet also folgende Gleichung statt:

$$\frac{\pi}{2} = q_1 - q_2 + q_3 - q_4 + \dots \pm q_{n+1}.$$

Aus der Abnahme der Glieder q_1, q_2, \dots folgt leicht, wenn man die Reihe bei ihrem $2m^{\text{ten}}$ und $(2m+1)^{\text{ten}}$ Gliede abbricht (wo natürlich $2m < n$):

$$(16) \quad \begin{cases} \frac{\pi}{2} > q_1 - q_2 + q_3 - \dots - q_{2m}, \\ \frac{\pi}{2} < q_1 - q_2 + q_3 - \dots - q_{2m} + q_{2m+1}. \end{cases}$$

Um sich zu überzeugen, dass diese Ungleichheiten stattfinden, darf man nur bemerken, dass im ersten Falle die weggebrachten Glieder, wenn man sie paarweise vereinigt, $q_{2m+1} - q_{2m+2}, q_{2m+3} - q_{2m+4}, \dots$ positive Differenzen geben, und dass man also etwas positives weglässt, und das Umgekehrte für den zweiten gilt.

Wir wenden uns jetzt zu der Betrachtung des Integrals:

$$\int_0^h \frac{\sin k\beta}{\sin \beta} f(\beta) d\beta = S,$$

wo h eine positive $\frac{\pi}{2}$ nicht übersteigende Constante und $f(\beta)$ eine stetige Function von β bezeichnet, welche, während β von 0 bis h wächst, immer positiv bleibt und nie zunimmt. Ich sage absichtlich, nie zunimmt, um den Fall nicht auszuschliessen, wo $f(\beta)$ stellenweise oder für das ganze Intervall constant bliebe. Der Buchstabe k ist nur zur Abkürzung für $2n+1$ eingeführt, und wir wollen untersuchen, wie sich S verändert, wenn n ohne Grenze wächst. Es sei $r\frac{\pi}{k}$ das grösste in h enthaltene Vielfache von $\frac{\pi}{k}$, wo offenbar die ganze Zahl r nicht grösser als n sein kann, und man zerlege das Integral in $r+1$ andre, zwischen den Grenzen 0 und $\frac{\pi}{k}, \frac{\pi}{k}, \dots, \frac{r\pi}{k}$ und h , so sind diese Integrale wieder abwechselnd positiv und negativ. Bezeichnet man dasjenige, welches die r^{te} Stelle einnimmt, abgesehen von seinem Zeichen,

mit R_r , so dass also:

$$R_r = \mp \int_{\frac{(r-1)\pi}{k}}^{\frac{r\pi}{k}} \frac{\sin k\beta}{\sin \beta} f(\beta) d\beta.$$

wo wieder das obere oder das untere Zeichen gilt, je nachdem r gerade oder ungerade ist, so hat man:

$$S = R_1 - R_2 + R_3 - \dots \pm R_{r+1}.$$

Die positiven Werthe R_1, R_2, R_3, \dots bilden eine abnehmende Reihe, wie man sich leicht überzeugt, wenn man auf R_r den Satz (8) anwendet. Man findet unter Berücksichtigung der über $f(\beta)$ gemachten Voraussetzung, dass:

$$R_r = \int_{\frac{(r-1)\pi}{k}}^{\frac{r\pi}{k}} \mp \frac{\sin k\beta}{\sin \beta} f(\beta) d\beta$$

zwischen den beiden Producten:

$$f\left(\frac{r\pi}{k}\right) \int_{\frac{(r-1)\pi}{k}}^{\frac{r\pi}{k}} \mp \frac{\sin k\beta}{\sin \beta} d\beta \quad \text{und} \quad f\left(\frac{(r-1)\pi}{k}\right) \int_{\frac{(r-1)\pi}{k}}^{\frac{r\pi}{k}} \mp \frac{\sin k\beta}{\sin \beta} d\beta$$

liegt, d. h. also:

$$R_r > q_r f\left(\frac{r\pi}{k}\right), \quad R_r < q_r f\left(\frac{(r-1)\pi}{k}\right).$$

Vergleicht man die untere Grenze $q_r f\left(\frac{r\pi}{k}\right)$ für R_r mit der oberen für R_{r+1} , welche $q_{r+1} f\left(\frac{r\pi}{k}\right)$ ist, so folgt wegen $q_r > q_{r+1}$, dass auch $R_r > R_{r+1}$, wie vorher behauptet wurde. Bricht man die Reihe S bei R_{2m} und R_{2m+1} ab (wo $2m < r$), so ergeben sich die Ungleichheiten:

$$S > R_1 - R_2 + R_3 - \dots - R_{2m}, \\ S < R_1 - R_2 + R_3 - \dots - R_{2m} + R_{2m+1}.$$

Die erste dieser Ungleichheiten wird nicht aufhören, richtig zu bleiben, wenn man statt der zu addirenden Glieder R_1, R_3, \dots ihre unteren Grenzen $q_1 f\left(\frac{\pi}{k}\right), q_3 f\left(\frac{3\pi}{k}\right), \dots$ und statt der zu subtrahirenden R_2, R_4, \dots ihre oberen

²⁾ Wäre $f\left(\frac{r\pi}{k}\right) = f\left(\frac{(r-1)\pi}{k}\right)$, so würden die beiden Grenzen zusammenfallen, und man muss um alle Fälle zu umfassen, mit dem Zeichen \pm den Sinn verbinden, dass \pm nicht kleiner als \pm ist.

Grenzen $q_2 f\left(\frac{\pi}{k}\right)$, $q_1 f\left(\frac{3\pi}{k}\right)$, ... setzt. Hierdurch und durch Anwendung des umgekehrten Verfahrens auf die untere Ungleichheit erhält man:

$$S > (q_1 - q_2) f\left(\frac{\pi}{k}\right) + (q_3 - q_1) f\left(\frac{3\pi}{k}\right) + \dots + (q_{2m-1} - q_{2m}) f\left(\frac{(2m-1)\pi}{k}\right),$$

$$S < q_1 f(0) - (q_2 - q_3) f\left(\frac{2\pi}{k}\right) - (q_4 - q_5) f\left(\frac{4\pi}{k}\right) - \dots - (q_{2m} - q_{2m+1}) f\left(\frac{2m\pi}{k}\right).$$

Da die Differenzen $q_1 - q_2$, $q_2 - q_3$, $q_3 - q_4$, ... positiv sind und die Function $f(\beta)$ nie zunimmt, so darf man offenbar in der ersten Ungleichheit $f\left(\frac{\pi}{k}\right)$, $f\left(\frac{3\pi}{k}\right)$, ... und in der zweiten $f\left(\frac{2\pi}{k}\right)$, $f\left(\frac{4\pi}{k}\right)$, ... mit $f\left(\frac{2m\pi}{k}\right)$ vertauschen. Es ist also:

$$S > (q_1 - q_2 + q_3 - \dots - q_{2m}) f\left(\frac{2m\pi}{k}\right),$$

$$S < q_1 f(0) - (q_2 - q_3 + q_4 - \dots - q_{2m+1}) f\left(\frac{2m\pi}{k}\right).$$

Die Zahl $2m$ ist kleiner als r , und also um so mehr kleiner als n , so dass die Resultate (16) stattfinden.

Die dort gefundenen Ungleichheiten lassen sich in die Form bringen:

$$q_2 - q_3 + \dots + q_{2m} > q_1 - \frac{\pi}{2}, \quad q_1 - q_2 + \dots - q_{2m} > \frac{\pi}{2} - q_{2m+1}.$$

Vergleicht man diese, nachdem man von beiden Seiten der ersten q_{2m+1} abgezogen hat, mit den vorher erhaltenen Grenzen für S , so ergeben sich folgende höchst einfache Resultate:

$$S > \frac{\pi}{2} f\left(\frac{2m\pi}{k}\right) - q_{2m+1} f\left(\frac{2m\pi}{k}\right),$$

$$S < \frac{\pi}{2} f\left(\frac{2m\pi}{k}\right) + q_{2m+1} f\left(\frac{2m\pi}{k}\right) + q_1 \left[f(0) - f\left(\frac{2m\pi}{k}\right) \right].$$

Unser Zweck war, die allmähliche Veränderung des Integrals:

$$S = \int_0^k \frac{\sin k\beta}{\sin \beta} f(\beta) d\beta$$

zu untersuchen, wenn man in demselben $k = 2n + 1$ nimmt und die ganze Zahl n über jede Grenze hinaus wachsen lässt. Diese Frage wird auf der Stelle durch die eben gefundenen Ausdrücke beantwortet. Nach dem Früheren ist die darin enthaltene gerade Zahl $2m$ für ein bestimmtes n insofern noch willkürlich, als sie

jeden r nicht übersteigenden Werth haben kann, wo r wie früher das grösste in $\frac{h}{\pi}k = \frac{h}{\pi}(2n+1)$ enthaltene Ganze bezeichnet. Da hiernach r offenbar gleichzeitig mit n über jede Grenze hinaus wächst, so darf auch $2m$ jede Grenze überschreiten.

Denkt man sich nun das gleichzeitige Wachsen von $2m$ und n so, dass dabei $\frac{2m}{k}$ successive jeden Grad von Kleinheit erreicht, so werden die für S gefundenen Grenzen zuletzt zusammenfallen. Betrachtet man zunächst die untere Grenze:

$$\frac{\pi}{2} f\left(\frac{2m\pi}{k}\right) - \varrho_{2m+1} f\left(\frac{2m\pi}{k}\right),$$

so wird unter der angegebenen Voraussetzung ihr erstes Glied zuletzt in $\frac{\pi}{2} f(0)$ übergehen; was das zweite betrifft, so liegt der Factor ϱ_{2m+1} nach Obigem zwischen:

$$\frac{1}{k} \frac{1}{\sin \frac{2m\pi}{k}} \quad \text{und} \quad \frac{1}{k} \frac{1}{\sin \frac{(2m+1)\pi}{k}}.$$

Schreibt man diese in folgender Form:

$$\frac{1}{2m\pi} \frac{2m\pi}{k} \sin \frac{2m\pi}{k} \quad \text{und} \quad \frac{1}{(2m+1)\pi} \frac{(2m+1)\pi}{k} \sin \frac{(2m+1)\pi}{k},$$

so ist leicht zu sehen, dass beide zuletzt verschwinden. Durch das unaufhörliche Wachsen von m nähert sich $\frac{1}{2m\pi}$ der Null, während $\frac{2m\pi}{k} \sin \frac{2m\pi}{k}$ wegen des Abnehmens von $\frac{2m\pi}{k}$ sich der Einheit nähert. Das Product wird also Null, und dasselbe gilt von dem zweiten. Es geht hieraus hervor, dass die untere Grenze für S zuletzt mit $\frac{\pi}{2} f(0)$ zusammenfällt. Die beiden ersten Glieder in der oberen Grenze sind den schon untersuchten ganz ähnlich, und es bleibt uns nur noch das dritte $\varrho_1 \left| f(0) - f\left(\frac{2m\pi}{k}\right) \right|$ zu betrachten. Der zweite Factor nähert sich offenbar der Null, und dieses Glied wird also verschwinden, wenn der erste nicht über jede Grenze hinaus wächst. Dass dieses

aber nicht der Fall ist, folgt sogleich aus den beiden Ungleichheiten:

$$q_1 < \frac{\pi}{2} + q_2, \quad q_2 < \frac{1}{k} \frac{1}{\sin \frac{\pi}{k}},$$

von denen die erste aus (16) hervorgeht, wenn man dort $m = 1$ setzt. Beide mit einander verglichen ergeben:

$$q_1 < \frac{\pi}{2} + \frac{1}{k} \frac{1}{\sin \frac{\pi}{k}},$$

und der Werth von:

$$\frac{1}{k} \frac{1}{\sin \frac{\pi}{k}} \quad \text{oder} \quad \frac{1}{\pi} \frac{k}{\sin \frac{\pi}{k}}$$

nähert sich durch das Wachsen von k dem Werthe $\frac{1}{\pi}$.

Es ist somit streng bewiesen, dass die beiden Grenzen, zwischen denen S eingeschlossen ist, bei unauflöflichem Wachsen von n zuletzt mit $\frac{\pi}{2} f(0)$ zusammenfallen, welcher Werth also auch der des Integrals:

$$\int_0^h \frac{\sin k\beta}{\sin \beta} f(\beta) d\beta$$

für ein unendlich grosses n ist.

Wir haben bisher vorausgesetzt, dass die Function $f(\beta)$, während β von 0 bis h wächst, nie zunimmt und ausserdem stets positiv bleibt. Behält man die erste Bedingung bei, d. h. setzt man voraus, dass für irgend zwei zwischen 0 und h fallende Werthe p und q die Differenz $f(p) - f(q)$ immer negativ oder Null ist, wenn $p - q$ positiv ist, ohne damit die zweite Annahme zu verbinden, dass $f(\beta)$ nicht negativ wird, so findet der vorige Satz ebenfalls noch statt. Nimmt man nämlich eine positive Constante c , welche so gross ist, dass $f(\beta) + c$ nicht negativ wird, so ist der Satz auf $f(\beta) + c$ anwendbar, d. h. das Integral:

$$\int_0^h [f(\beta) + c] \frac{\sin k\beta}{\sin \beta} d\beta$$

wird für ein unendlich grosses n :

$$\frac{\pi}{2} [f(0) + c].$$

Zugleich ist klar, dass dieses Integral die Summe von folgenden ist:

$$\int_0^h f(\beta) \frac{\sin k\beta}{\sin \beta} d\beta, \quad \int_0^h c \frac{\sin k\beta}{\sin \beta} d\beta,$$

von denen das zweite in demselben Falle $\frac{\pi}{2} c$ wird. (Es ist nämlich bei der vorigen Behandlung der Fall mit eingeschlossen worden, wo die positive Function im ganzen Intervall constant war). Also muss das erste durch unaufhörliches Wachsen von n zuletzt den Werth $\frac{\pi}{2} f(0)$ annehmen.

Denkt man sich jetzt eine Function $f(\beta)$, die, während β von 0 bis h wächst, nie abnimmt, so wird $-f(\beta)$ nie zunehmen. Man hat also, wenn n unendlich wächst:

$$\int_0^h -f(\beta) \frac{\sin k\beta}{\sin \beta} d\beta = -\frac{\pi}{2} f(0)$$

und folglich:

$$\int_0^h f(\beta) \frac{\sin k\beta}{\sin \beta} d\beta = \frac{\pi}{2} f(0).$$

Die vorhergehenden Resultate lassen sich in folgenden Satz zusammenfassen:

(17) Ist $f(\beta)$ eine stetige Function von β , die, während β von 0 bis h wächst (wo die Constante $h > 0$ und $< \frac{\pi}{2}$), nie vom Abnehmen ins Zunehmen oder umgekehrt übergeht, so wird das Integral:

$$\int_0^h \frac{\sin(2n+1)\beta}{\sin \beta} f(\beta) d\beta,$$

wenn man darin der ganzen Zahl n immer grössere positive Werthe beilegt, zuletzt immerfort weniger als jede angebbare Grösse von $\frac{\pi}{2} f(0)$ verschieden sein.

Die Constante h bleibe den vorigen Bestimmungen unterworfen und man denke sich unter g eine zweite Constante, welche kleiner als h und zugleich positiv und von Null verschieden sei. Ist $f(\beta)$ eine für das Intervall von g bis h gegebene stetige Function von β , die, wenn β von g bis h wächst, nie vom Abnehmen ins Zunehmen oder umgekehrt übergeht, so lässt sich nach dem vorigen Satz leicht ermitteln, was aus dem Integral:

$$\int_g^h \frac{\sin(2n+1)\beta}{\sin \beta} f(\beta) d\beta$$

wird, wenn man n unendlich werden lässt. Da nämlich $f(\beta)$ bloss von $\beta = g$ bis $\beta = h$ gegeben ist, so bleibt die Art der Fortsetzung dieser Function über das genannte Intervall hinaus ganz willkürlich. Denkt man sich $f(\beta)$ für alle Werthe von β zwischen 0 und g incl. constant, und zwar $= f(g)$, so hat man eine von $\beta = 0$ bis $\beta = h$ stetige Function, welche in diesem ganzen Intervall nie vom Abnehmen ins Zunehmen oder umgekehrt übergeht, und auf welche daher der vorige Satz anwendbar ist. Es wird daher das Integral:

$$\int_0^h \frac{\sin(2n+1)\beta}{\sin\beta} f(\beta) d\beta,$$

wenn man $n = \infty$ setzt, $= \frac{\pi}{2} f(0) = \frac{\pi}{2} f(g)$ sein. Zerlegt man dasselbe Integral in die folgenden:

$$\int_0^g \frac{\sin(2n+1)\beta}{\sin\beta} f(\beta) d\beta + \int_g^h \frac{\sin(2n+1)\beta}{\sin\beta} f(\beta) d\beta$$

so wird auch das erste $= \frac{\pi}{2} f(0) = \frac{\pi}{2} f(g)$ nach dem vorigen Satz, also muss das zweite für ein unendliches n verschwinden. Es gilt also der Satz:

(18) $\left\{ \begin{array}{l} \text{Sind } g \text{ und } h \text{ Constanten, welche den Bedingungen genügen } g > 0, \\ \frac{\pi}{2} \geq h > g, \text{ und geht die Function } f(\beta), \text{ wenn } \beta \text{ von } g \text{ bis } h \text{ wächst,} \\ \text{nie vom Abnehmen ins Zunehmen oder umgekehrt über, so wird das} \\ \text{Integral:} \\ \int_g^h \frac{\sin(2n+1)\beta}{\sin\beta} f(\beta) d\beta \\ \text{für ein unendlich grosses } n \text{ der Null gleich.} \end{array} \right.$

Vermittelst der Sätze (17) und (18) ist es nun leicht, die zu Ende des §. 4. aufgestellte Behauptung zu beweisen.

§. 6.

Die Summe der $2n+1$ ersten Glieder der zu untersuchenden Reihe war durch das Integral:

$$\frac{1}{\pi} \int_{-\pi}^{+\pi} d\beta q(\beta) \frac{\sin(2n+1) \frac{\beta-x}{2}}{2 \sin \frac{\beta-x}{2}}$$

ausgedrückt. Wir haben früher vorausgesetzt, dass die Function $g(\beta)$ für das ganze Intervall von $\beta = -\pi$ bis $\beta = \pi$ stetig ist; wir können aber, ohne die folgende Untersuchung im Geringsten zu erschweren, die Annahme machen, dass $g(\beta)$ für einzelne Werthe von β eine plötzliche Veränderung erleidet, ohne jedoch unendlich zu werden. Die Curve, deren Abscisse β und deren Ordinate $g(\beta)$ ist, besteht alsdann aus mehreren Stücken, deren Zusammenhang über den Punkten der Abscissenaxe, die jenen besonderen Werthen von β entsprechen, unterbrochen ist, und für jede solche Abscisse finden eigentlich zwei Ordinaten statt, wovon die eine dem dort endenden und die andere dem dort beginnenden Curvenstück angehört. Es wird im Folgenden nöthig sein, diese beiden Werthe von $g(\beta)$ zu unterscheiden, und wir werden sie durch $g(\beta-0)$ und $g(\beta+0)$ bezeichnen. Um unnütze, die folgende Darstellung verlängernde Unterscheidungen zu vermeiden, bemerke man, dass dieselbe Bezeichnung auch für die Werthe von β gelten kann, für welche keine Unterbrechung der Stetigkeit stattfindet, wo dann natürlich $g(\beta-0)$ und $g(\beta+0)$ beide mit $g(\beta)$ gleichbedeutend sind.

Das obige Integral lässt sich nach (9) in die folgenden zerlegen:

$$\frac{1}{\pi} \int_{-\pi}^{+\pi} d\beta g(\beta) \frac{\sin(2n+1) \frac{\beta-x}{2}}{2 \sin \frac{\beta-x}{2}}, \quad \frac{1}{\pi} \int_x^{\pi} d\beta g(\beta) \frac{\sin(2n+1) \frac{\beta-x}{2}}{2 \sin \frac{\beta-x}{2}}$$

oder nach (4):

$$\frac{1}{\pi} \int_{(x+x)}^{+0} d\beta g(x+\beta) \frac{\sin(2n+1) \frac{\beta}{2}}{2 \sin \frac{\beta}{2}}, \quad \frac{1}{\pi} \int_0^{+\pi-x} d\beta g(x+\beta) \frac{\sin(2n+1) \frac{\beta}{2}}{2 \sin \frac{\beta}{2}}.$$

Wendet man (3) auf beide an und nachher noch (2) und (5) auf das erste, so kommt:

$$(19) \quad \frac{1}{\pi} \int_0^{+\pi-x} d\beta g(x-2\beta) \frac{\sin(2n+1)\beta}{\sin \beta}, \quad \frac{1}{\pi} \int_0^{+\pi-x} d\beta g(x+2\beta) \frac{\sin(2n+1)\beta}{\sin \beta}.$$

Wir betrachten jetzt das zweite dieser Integrale, abgesehen von dem constanten Factor $\frac{1}{\pi}$. Da x zwischen $-\pi$ und $+\pi$ liegt, so liegt $\frac{\pi-x}{2}$ zwischen 0 und π . Ist $\frac{\pi-x}{2} = 0$, was für $x = \pi$ der Fall ist, so ist das Inte-

gral für jedes n Null und erfordert keine weitere Untersuchung. Nehmen wir zunächst an, $\frac{\pi-x}{2}$ sei nicht grösser als $\frac{\pi}{2}$. Man bezeichne mit e_1, e_2, \dots, e_r , wie sie der Grösse nach auf einander folgen, die Werthe von β , für welche *erstens* $g(x+2\beta)$ innerhalb des Intervalls von $\beta=0$ bis $\beta=\frac{\pi-x}{2}$ eine Unterbrechung der Stetigkeit erleidet und *zweitens* vom Zunehmen ins Abnehmen oder vom Abnehmen ins Zunehmen übergeht, und zerlege das Integral in andere zwischen den Grenzen 0 und e_1, e_1 und e_2, \dots, e_r und $\frac{\pi-x}{2}$ genommen. Auf alle diese neuen Integrale, mit Ausnahme des ersten, ist der Satz (18) offenbar anwendbar, da innerhalb der Grenze eines jeden die Function keine Unterbrechung der Stetigkeit erleidet und nicht vom Abnehmen ins Zunehmen oder umgekehrt übergeht; alle nähern sich daher ins Unendliche der Null, wenn man n über alle Grenzen hinaus wachsen lässt. Das erste hingegen erfüllt die Bedingungen (17) und geht bei unaufhörlichem Wachsen von n zuletzt in den Werth $\frac{\pi}{2} g(x+0)$ über. Also wird das Integral:

$$\int_0^{\frac{\pi-x}{2}} d\beta g(x+2\beta) \cdot \frac{\sin(2n+1)\beta}{\sin\beta}$$

für $n = \infty$ den Werth $\frac{\pi}{2} g(x+0)$ annehmen.

Liegt $\frac{\pi-x}{2}$ über $\frac{\pi}{2}$ oder ist x negativ, so zerlege man das vorige Integral in zwei andere zwischen den Grenzen 0 und $\frac{\pi}{2}, \frac{\pi}{2}$ und $\frac{\pi-x}{2}$. Auf das erste dieser neuen Integrale bleibt das vorige Verfahren anwendbar, und dasselbe wird also $\frac{\pi}{2} g(x+0)$, wenn man n unendlich gross werden lässt. Das andere:

$$\int_{\frac{\pi}{2}}^{\frac{\pi-x}{2}} d\beta g(x+2\beta) \cdot \frac{\sin(2n+1)\beta}{\sin\beta}$$

kann nach (4) und (5) in die Form gebracht werden:

$$-\int_{\frac{\pi}{2}}^{\frac{(\pi+x)}{2}} d\beta g(x+2\pi-2\beta) \cdot \frac{\sin(2n+1)(\pi-\beta)}{\sin(\pi-\beta)}.$$

Wendet man (2) an, und setzt $\sin\beta$ statt $\sin(\pi-\beta)$ und $\sin(2n+1)\beta$ statt $\sin(2n+1)(\pi-\beta)$ (da n eine ganze Zahl ist), so geht das Integral über in:

$$\int_{\frac{\pi+x}{2}}^{\frac{x}{2}} g(x+2\pi-2\beta) \frac{\sin(2n+1)\beta}{\sin\beta} d\beta.$$

Da x , wie vorher gesagt wurde, in diesem Falle negativ ist und also zwischen 0 und $-\pi$ liegt, so ist $\frac{\pi+x}{2}$ positiv und von Null verschieden, den einzigen Fall ausgenommen, wo $x = -\pi$. Zerlegt man das Integral in andere, zwischen deren Grenzen $g(x+2\pi-2\beta)$ weder eine Unterbrechung der Continuität erleidet noch aus dem Zunehmen ins Abnehmen oder umgekehrt übergeht, so werden alle diese Integrale nach (18) für $n = \infty$ der Null gleich. Dieses Resultat gilt nicht, wenn $\frac{\pi+x}{2} = 0$ und also $x = -\pi$, da alsdann auf das erste der durch Zerlegung entstehenden Integrale nicht der Satz (18) sondern der Satz (17) angewendet werden muss. Dieses erste Integral ist alsdann (wegen $x = -\pi$):

$$\int_0^{\pi} d\beta g(x+2\pi-2\beta) \frac{\sin(2n+1)\beta}{\sin\beta} = \int_0^{\pi} d\beta g(\pi-2\beta) \frac{\sin(2n+1)\beta}{\sin\beta}$$

und wird also für $n = \infty$ den Werth $\frac{\pi}{2} g(\pi-0)$ erhalten, während alle übrigen verschwinden.

Vereinigt man die verschiedenen für das zweite Integral (19) gefundenen Resultate, so ergibt sich, dass dieses Integral durch unaufhörliches Wachsen der darin enthaltenen ganzen Zahl n für jedes zwischen $-\pi$ und $+\pi$ gelegene x in den Werth $\frac{1}{2}g(x+0)$ übergeht. Für $x = \pi$ und $x = -\pi$ erleidet das Resultat eine Ausnahme: in dem erstern Falle ist das Integral Null, im andern wird es $\frac{1}{2}[g(\pi-0) + g(-\pi+0)]$. Aus einer ganz ähnlichen Untersuchung des ersten Integrals (19) folgt, dass dasselbe für $n = \infty$ im Allgemeinen $\frac{1}{2}g(x-0)$ wird, aber in den besondern Fällen, $x = -\pi$ und $x = \pi$, respective Null und $\frac{1}{2}[g(\pi-0) + g(-\pi+0)]$.

Ermindert man sich nun, dass die beiden Integrale (19) zusammengenommen die Summe der $2n+1$ ersten Glieder der Reihe darstellen:

$$(20) \quad \begin{aligned} & \frac{1}{2} b_0 + b_1 \cos x + b_2 \cos 2x + \dots + b_m \cos mx + \dots \\ & + a_1 \sin x + a_2 \sin 2x + \dots + a_m \sin mx + \dots, \end{aligned}$$

wo die Coefficienten durch die Gleichungen:

$$b_m = \frac{1}{\pi} \int_{-\pi}^{+\pi} d\beta g(\beta) \cos m\beta, \quad a_m = \frac{1}{\pi} \int_{-\pi}^{+\pi} d\beta g(\beta) \sin m\beta$$

zu bestimmen sind, so geht aus dem Vorhergehenden ganz streng hervor, dass diese Reihe immer convergirt, d. h. dass es immer einen gewissen Werth giebt, von dem die Summe der $2n+1$ ersten Glieder der Reihe, wenn n über alle Grenzen hinaus wachsend gedacht wird, zuletzt immerfort um weniger als jede angebbare Grösse verschieden sein wird, und dass dieser Werth oder die Summe der unendlichen Reihe, wenn x zwischen $-\pi$ und π liegt, durch $\frac{1}{2}[g(x+0)+g(x-0)]$, für $x = \pi$ und $x = -\pi$ aber durch $\frac{1}{2}[g(\pi-0)+g(-\pi+0)]$ dargestellt wird.

Dieses Resultat umfasst alle Fälle: ist x keiner von den besondern Werthen, für welche die Stetigkeit von $g(x)$ unterbrochen wird, so sind $g(x+0)$ und $g(x-0)$ einander gleich, und der Werth der Reihe wird also $g(x)$. Wo eine Unterbrechung der Stetigkeit eintritt und also die Function $g(x)$ eigentlich zwei Werthe hat, stellt die Reihe, welche ihrer Natur nach für jedes x einwerthig ist, die halbe Summe dieser Werthe dar. An den Grenzen des Intervalls von $-\pi$ bis $+\pi$, d. h. für diese Werthe selbst, ist die Summe der unendlichen Reihe gleich der halben Summe der beiden Werthe $g(\pi)$ und $g(-\pi)$. Man sieht daraus, dass die Reihe die Function $g(x)$ an den Grenzen des Intervalls nur dann richtig darstellt, wenn $g(\pi) = g(-\pi)$ ist.

Wir haben schon früher bemerkt, dass die eben untersuchte Reihe (20) oder (15) die Reihen (13) und (14) als specielle Fälle in sich begreift. Man braucht sich nur die Function $g(x)$ für den halben Umfang des Intervalls, nämlich $x = 0$ bis $x = \pi$, als ganz beliebig gegeben zu denken und für die Werthe zwischen 0 und $-\pi$ fortgesetzt zu denken, wie es die Gleichungen $g(-x) = g(x)$ oder $g(-x) = -g(x)$ vorschreiben, um respective zu (14) und (13) zu gelangen. Ich will dies noch mit zwei Worten für den ersten Fall zeigen, weil sich aus dieser Ableitung eine Eigenschaft der Reihe (14) ergibt, welche bei der frühern Behandlung nicht hervortrat.

Setzt man die von 0 bis π beliebige Function $g(x)$ nach der Gleichung $g(-x) = g(x)$ fort, so ist klar, dass für $x = 0$ keine Unterbrechung der Stetigkeit eintreten und dass $g(-\pi) = g(\pi)$ sein wird. Die Reihe (20) wird also $g(0)$ für $x = 0$, und $g(\pi)$ für $x = \pi$. Die Gleichungen für die Coefficienten

werden durch Zerlegung der darin enthaltenen Integrale:

$$b_m = \frac{1}{\pi} \int_{-\pi}^0 d\beta g(\beta) \cos m\beta + \frac{1}{\pi} \int_0^{\pi} d\beta g(\beta) \cos m\beta,$$

$$a_m = \frac{1}{\pi} \int_{-\pi}^0 d\beta g(\beta) \sin m\beta + \frac{1}{\pi} \int_0^{\pi} d\beta g(\beta) \sin m\beta.$$

Wendet man auf die beiden von $-\pi$ bis 0 genommenen Integrale nach einander (5) und (2) an und berücksichtigt, dass:

$$g(-\beta) = g(\beta), \quad \cos(-m\beta) = \cos m\beta, \quad \sin(-m\beta) = -\sin m\beta,$$

so erhält man:

$$b_m = \frac{2}{\pi} \int_0^{\pi} d\beta g(\beta) \cos m\beta, \quad a_m = 0.$$

Die von $x=0$ bis $x=\pi$ ganz beliebig gegebene Function $g(x)$ wird also durch die Reihe:

$$\frac{1}{2}b_0 + b_1 \cos x + b_2 \cos 2x + \dots + b_m \cos mx + \dots$$

dargestellt, welche auch für die das Intervall begrenzenden Werthe 0 und π noch gültig ist. Es versteht sich dabei von selbst, dass, wenn $g(x)$ zwischen 0 und π eine Unterbrechung der Stetigkeit erleidet, die Reihe für jeden solchen Werth von x die halbe Summe der entsprechenden Werthe von $g(x)$ ausdrückt. Auf ganz ähnliche Weise gelangt man zu der Reihe (13) und findet, dass diese im Allgemeinen für $x=0$ und $x=\pi$ nicht mehr richtig ist, was sich aber in diesem Fall ganz von selbst versteht, da die Reihe, wie auch ihre Coefficienten beschaffen sein mögen, für die genannten Werthe verschwindet.

SOLUTION D'UNE QUESTION RELATIVE A LA THÉORIE MATHÉMATIQUE DE LA CHALEUR.

PAR

M. G. LEJEUNE DIRICHLET,
PROF. DE MATH.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 5 p. 287 — 295.

SOLUTION D'UNE QUESTION RELATIVE A LA THÉORIE MATHÉMATIQUE DE LA CHALEUR.

La question qui va nous occuper et qui a pour objet de déterminer les états successifs d'une barre primitivement échauffée d'une manière quelconque et dont les deux extrémités sont entretenues à des températures données en fonction du temps, a déjà été résolue par M. FOURIER dans un Mémoire inséré dans le Vol. VIII de la collection de l'Académie Royale des Sciences de Paris. La méthode dont cet illustre géomètre a fait usage dans cette recherche est une espèce singulière de passage du fini à l'infini, et offre un nouvel exemple de la fécondité de ce procédé analytique qui avait déjà conduit l'auteur à tant de résultats remarquables dans son grand ouvrage sur la théorie de la chaleur. J'ai traité la même question par une analyse dont la marche diffère beaucoup de celle de M. FOURIER et qui donne lieu à l'emploi de quelques artifices de calcul, qui paraissent pouvoir être utiles dans d'autres recherches.

Pour simplifier les calculs, nous supposerons l'unité linéaire qui est arbitraire, tellement choisie que la longueur de la barre soit égale à π , cette lettre désignant à l'ordinaire le rapport du diamètre à la circonférence. Soit x la distance d'un point quelconque de la barre à l'une de ses extrémités, que nous nommerons la première extrémité. La température du point x à l'instant t est une fonction u de x et de t , et c'est cette fonction qui fait l'objet de la question. Soit $F(t)$ la fonction donnée de t qui exprime la température à laquelle la première extrémité est entretenue, et soit de même $f(t)$ la température de la seconde extrémité, $F(t)$ et $f(t)$ étant des fonctions arbitraires dont les valeurs sont données pour toute valeur positive de t , et désignons enfin par $g(x)$ la température initiale du point dont l'abscisse est x .

En faisant abstraction du rayonnement latéral, la fonction u doit satisfaire à cette équation aux différences partielles $\frac{\partial u}{\partial t} = k \frac{\partial^2 u}{\partial x^2}$ dans laquelle k désigne un coefficient dépendant des propriétés spécifiques de la substance dont la barre est formée.

Pour plus de simplicité, nous supposons égal à l'unité le coefficient k qu'il sera facile de rétablir à la fin du calcul, de sorte que l'équation précédente se changera en celle-ci :

$$(1) \quad \frac{\partial u}{\partial t} = \frac{\partial^2 u}{\partial x^2} .$$

Cela posé, la fonction cherchée doit évidemment remplir les quatre conditions suivantes :

- $$(2) \quad \left\{ \begin{array}{l} 1^{\circ}. \text{ Elle doit satisfaire à l'équation (1) quels que soient } x \text{ et } t. \\ 2^{\circ}. \text{ Pour } x = 0, \text{ elle doit se réduire à la fonction donnée } F(t). \\ 3^{\circ}. \text{ Pour } x = \pi, \text{ elle doit se réduire à la fonction } f(t) \text{ également} \\ \text{donnée.} \\ 4^{\circ}. \text{ Lorsque } t \text{ est nul, elle doit coïncider dans toute l'étendue de la} \\ \text{barre, c'est-à-dire tant que } x \text{ est inférieur à } \pi, \text{ avec la fonction} \\ g(x) \text{ qui exprime les températures initiales.} \end{array} \right.$$

La question que nous avons à résoudre se partage naturellement en deux autres. On fera d'abord abstraction de la quatrième condition et l'on cherchera une fonction v de x et de t uniquement assujettie à remplir les 3 premières. Il y a une infinité de fonctions qui satisfont à ces 3 conditions, et qui diffèrent entre elles en ce qu'elles se réduisent à des fonctions de x différentes entre elles par la supposition de $t = 0$; mais il suffit d'en obtenir une seule. Une pareille fonction v étant trouvée, on y fera $t = 0$, ce qui la réduira à une fonction $\chi(x)$ de x . On formera ensuite la différence $g(x) - \chi(x)$ et l'on cherchera la fonction entièrement déterminée w de x et de t , qui satisfait à l'équation (1), s'évanouit pour $x = 0$ et $x = \pi$ quel que soit t , et se réduit à $g(x) - \chi(x)$ lorsqu'on y fait $t = 0$.

Cette seconde question est résolue depuis longtemps, c'est celle de la détermination du mouvement de la chaleur dans une barre dont l'état initial est exprimé par $g(x) - \chi(x)$ et dont les extrémités sont entretenues à la température zéro. Les deux fonctions v et w dont il vient d'être question, étant

ajoutées, formeront une nouvelle fonction de x et de t , qui remplit l'ensemble des conditions (2). En effet, chacune d'elles satisfaisant à l'équation (1), leur somme y satisfera également. La première se réduisant à $F(t)$ pour $x = 0$, et la seconde s'évanouissant dans cette même supposition, leur somme remplira évidemment la seconde des conditions (2). Il en est de même de la troisième de ces conditions. Quant à la quatrième, il est également manifeste qu'elle est satisfaite par la somme $v+w$ que nous venons de former, v se réduisant à $\chi(x)$ et w à $g(x)-\chi(x)$, lorsqu'on y suppose le temps nul. La somme $v+w$ est donc la fonction cherchée u .

La marche que nous venons d'indiquer revient à assujettir les deux extrémités d'une barre, l'une à la température $F(t)$, l'autre à la température $f(t)$, sans supposer arbitraire l'état initial de cette barre, à considérer une seconde barre dont les extrémités sont entretenues à la température zéro et dont l'état initial est la différence entre l'état initial arbitraire $g(x)$ et celui de la première barre, et à ajouter ensuite les expressions qui expriment les états variables de ces deux barres.

La recherche de la fonction v peut à son tour se décomposer en deux autres questions plus simples: car il est évident que pour obtenir une fonction qui remplisse les 3 premières des conditions (2), il suffit de chercher d'abord une expression v' qui soit assujettie à la première et à la troisième de ces conditions et qui s'évanouisse pour $x = 0$, et de déterminer ensuite une seconde expression v'' qui remplisse la première et la seconde, et devienne égale à zéro lorsqu'on y suppose $x = \pi$: la somme $v'+v''$ de ces expressions satisfera manifestement aux 3 premières des conditions (2), et pourra par conséquent être prise pour v .

Quant à ces nouvelles fonctions v' et v'' , il est facile de voir qu'elles peuvent être obtenues de la même manière, c'est-à-dire que l'une d'elles, la première v' par exemple, étant trouvée, l'autre v'' s'en déduira immédiatement. Il suffira pour cela, de changer en $F(t)$ la fonction arbitraire $f(t)$ que renferme cette expression v' et d'y remplacer en même temps x par $\pi-x$. Il est évident que l'expression v' ainsi modifiée satisfera toujours à l'équation (1) et que pour $x = 0$, $x = \pi$ elle se réduira respectivement à $F(t)$ et à zéro; elle pourra donc être prise pour v'' .

Toute la difficulté du problème que nous nous sommes proposé de résoudre, se réduit donc à la recherche d'une fonction v' de x et de t , qui rem-

plisse les 3 conditions de satisfaire à l'équation (1), de s'évanouir pour $x = 0$, et de se réduire à $f(t)$ lorsqu'on y fait $x = \pi$.

On satisfait à l'équation:

$$\frac{\partial u}{\partial t} = \frac{\partial^2 u}{\partial x^2}$$

par une solution particulière de cette forme:

$$(3) \quad r \cos at + s \sin at,$$

a désignant une quantité constante mais arbitraire, et r et s étant des fonctions de x et de a sans t . En effet, différentiant l'expression précédente une fois par rapport à t , et deux fois par rapport à x , et égalant les deux résultats, il viendra:

$$\frac{\partial^2 r}{\partial x^2} \cos at + \frac{\partial^2 s}{\partial x^2} \sin at = a s \cos at - a r \sin at,$$

équation qui aura évidemment lieu quels que soient x et t , si les fonctions r et s sont telles que l'on ait:

$$(4) \quad \frac{\partial^2 r}{\partial x^2} = a s, \quad \frac{\partial^2 s}{\partial x^2} = -a r.$$

Ces équations différentielles simultanées étant linéaires et à coefficients constants, il sera facile d'en trouver les intégrales complètes, et comme ces équations sont l'une et l'autre du second ordre, les valeurs générales de r et de s renfermeront chacune deux constantes arbitraires. Ces 4 constantes peuvent servir à assujettir chacune des fonctions r et s à deux conditions. Supposons qu'on les choisisse de manière à avoir $r = 0$, $s = 0$ lorsque $x = 0$, et $r = 1$, $s = 0$ lorsqu'on fait $x = \pi$. Désignant par R et S les valeurs de r et s ainsi particularisées, nous aurons l'expression:

$$(5) \quad R \cos at + S \sin at$$

qui, outre qu'elle satisfait à l'équation:

$$\frac{\partial u}{\partial t} = \frac{\partial^2 u}{\partial x^2}$$

jouit encore de la double propriété de s'évanouir pour $x = 0$, et de se réduire à $\cos at$, lorsqu'on y fait $x = \pi$. L'expression précédente étant multipliée par $\psi(a) da$, $\psi(a)$ désignant une fonction entièrement arbitraire de a , et intégrée

depuis $\alpha = 0$ jusqu'à $\alpha = \infty$, donnera cette nouvelle fonction de x et de t :

$$\int_0^{\infty} (R \cos \alpha t + S \sin \alpha t) \psi(\alpha) d\alpha,$$

qui satisfera également à l'équation:

$$\frac{\partial u}{\partial t} = \frac{\partial^2 u}{\partial x^2},$$

s'évanouira pour $x = 0$, et deviendra:

$$\int_0^{\infty} \psi(\alpha) \cos \alpha t d\alpha.$$

lorsqu'on y fait $x = \pi$. La fonction $\psi(\alpha)$ étant arbitraire, on peut la choisir de manière que l'intégrale précédente devienne égale à la fonction donnée $f(t)$, pour toute valeur positive de t . La fonction $\psi(\alpha)$ qui remplit cette condition, est d'après le théorème connu de M. FOURIER (*Théorie de la chaleur*, art. 346, pag. 431) celle que donne l'équation:

$$\psi(\alpha) = \frac{2}{\pi} \int_0^{\infty} \cos \alpha \mu f(\mu) d\mu,$$

dans laquelle μ est une variable auxiliaire qui disparaît par l'intégration définie. Si l'on substitue cette valeur de $\psi(\alpha)$ dans l'expression obtenue plus haut, on aura cette nouvelle expression:

$$(6) \quad \frac{2}{\pi} \int_0^{\infty} \int_0^{\infty} (R \cos \alpha t + S \sin \alpha t) f(\mu) \cos \alpha \mu d\alpha d\mu,$$

qui remplit les 3 conditions de satisfaire à l'équation:

$$\frac{\partial u}{\partial t} = \frac{\partial^2 u}{\partial x^2},$$

de s'évanouir pour $x = 0$, et de devenir $f(t)$ pour $x = \pi$. Cette expression peut donc être prise pour v' . Si l'on change ensuite x en $\pi - x$, et $f(\mu)$ en $F(\mu)$ dans l'expression précédente, on aura une nouvelle expression, que l'on pourra prendre pour v'' , et il ne restera plus qu'à former la troisième partie w de la solution.

Cette troisième partie exprime, comme nous l'avons vu plus haut, les états successifs d'une barre dont les deux extrémités sont entretenues à la température zéro et dont l'état initial est $\varphi(x) - \chi(x)$, $\varphi(x)$ étant une fonction

primitivement donnée et $\chi(x)$ désignant la fonction de x , à laquelle se réduit la somme $v' + v'' = v$, lorsqu'on y fait $t = 0$. Quoique, d'après ce que nous avons dit plus haut, il suffise pour la solution de notre problème, d'obtenir une quelconque des fonctions en nombre infini qui remplissent les 3 premières des conditions (2), le choix de cette fonction n'est pas indifférent. Le calcul se simplifie d'une manière remarquable, lorsque l'on prend pour v une fonction telle que l'on puisse prévoir, quelle est la fonction $\chi(x)$ à laquelle elle se réduit pour $t = 0$: car alors on pourra former immédiatement la troisième partie u , dans la composition de laquelle entre cette fonction $\chi(x)$. La valeur de v précédemment obtenue ne présente pas cette facilité, mais il est facile d'en obtenir une qui remplisse cet objet, en modifiant un peu l'analyse que nous venons d'employer. C'est ce que nous allons faire voir en reprenant ce que nous avons dit depuis que nous sommes parvenu à l'expression (5).

La variable t étant remplacée dans cette expression par $t - \mu$, μ désignant une nouvelle arbitraire indépendante de α , x et t , elle ne cessera pas de satisfaire à l'équation:

$$\frac{\partial u}{\partial t} = \frac{\partial^2 u}{\partial x^2}$$

et de s'évanouir pour $x = 0$, quelle que soit la valeur positive ou négative de t , mais pour $x = \pi$ elle se réduira à $\cos \alpha(t - \mu)$.

Multipliant l'expression ainsi modifiée par $\frac{1}{\pi} f(\mu) d\alpha d\mu$ et intégrant depuis $\mu = 0$, $\alpha = 0$, jusqu'à $\mu = \infty$, $\alpha = \infty$, on aura cette nouvelle fonction de x et de t :

$$(7) \quad \frac{1}{\pi} \int_0^{\infty} \int_0^{\infty} (R \cos \alpha(t - \mu) + S \sin \alpha(t - \mu)) f(\mu) d\alpha d\mu,$$

qui satisfait encore à l'équation:

$$\frac{\partial u}{\partial t} = \frac{\partial^2 u}{\partial x^2}$$

s'évanouit pour $x = 0$, et se réduit à:

$$\frac{1}{\pi} \int_0^x \int_0^{\infty} \cos \alpha(t - \mu) f(\mu) d\alpha d\mu,$$

lorsqu'on y fait $x = \pi$. La valeur de cette intégrale double est connue par le

théorème de M. FOURIER et l'intégration relative à μ ne s'étendant que depuis $\mu = 0$ jusqu'à $\mu = \infty$, cette valeur est $f(t)$ lorsque t est positif, et égale à zéro lorsque le temps t devient négatif. La formule (7) exprime donc les états variables d'une barre dont les deux extrémités ont été entretenues à la température zéro pendant tout le temps infini antérieur à l'instant qui répond à $t = 0$, et dont la seconde extrémité est entretenue à la température $f(t)$ à partir de cette époque, la première conservant toujours la température zéro. Or il est évident qu'une barre dont les deux extrémités ont été assujetties à la température zéro pendant un temps infini, a acquis dans tous ses points cette même température zéro. Donc, l'expression (7) doit s'évanouir pour toute valeur de x inférieure à π , lorsqu'on y fait $t = 0$. Il serait d'ailleurs facile d'obtenir cette même conséquence par le seul examen de l'expression (7) et sans aucune considération physique.

Prenant l'expression (7) pour v' et l'expression qui s'en déduit par le changement de $f(\mu)$ en $F(\mu)$ et de x en $\pi - x$, pour v'' , la somme $v' + v''$ s'évanouira pour $t = 0$: la fonction $\chi(x)$ sera nulle et la troisième partie w sera l'expression des états variables d'une barre dont les deux extrémités sont assujetties à la température zéro et dont l'état initial est exprimé par la fonction connue $g(x)$. Cette troisième partie w est donnée par la formule suivante, dans laquelle le signe Σ se rapporte à toutes les valeurs positives et entières de i :

$$\frac{2}{\pi} \Sigma e^{-i^2 t} \sin i x \int_0^{\pi} g(\mu) \sin i \mu d\mu,$$

(Théorie de la chaleur, art. 252, pag. 436).

La valeur de v' (7) est sous une forme assez compliquée. Il en est de même de la seconde partie v'' . Ces deux expressions se simplifient beaucoup lorsqu'on leur donne une forme analogue à celle de la troisième, c'est-à-dire, lorsqu'on les développe en séries de sinus des arcs multiples de x . Ce développement est évidemment permis, la variable x ne devant recevoir que des valeurs inférieures à π dans l'expression v' (7) et dans l'expression analogue v'' . Pour transformer la fonction (7) en une pareille série, il suffira de développer R et S qui renferment seules la variable x . Faisons donc:

$$(8) \quad R = \Sigma b_i \sin i x, \quad S = \Sigma c_i \sin i x$$

le signe Σ se rapportant comme précédemment aux valeurs positives et entières

de i . Les coefficients b_i et c_i qui ne peuvent dépendre que de a , seront donnés par ces intégrales définies, d'après la théorie connue des séries de sinus :

$$(9) \quad b_i = \frac{2}{\pi} \int_0^\pi R \sin i x dx, \quad c_i = \frac{2}{\pi} \int_0^\pi S \sin i x dx.$$

On peut obtenir les valeurs de ces deux intégrales définies sans être obligé de résoudre les équations différentielles (4).

Pour y parvenir, nous remplacerons dans les expressions précédentes de b_i et c_i , R et S par les différentielles secondes $-\frac{1}{a} \cdot \frac{\partial^2 S}{\partial x^2}$, $\frac{1}{a} \cdot \frac{\partial^2 R}{\partial x^2}$ qui leur sont respectivement égales en vertu des équations (4) dont R et S sont des intégrales particulières. Intégrant ensuite deux fois par parties les expressions de b_i et c_i , et observant qu'à la première limite $x = 0$, $\sin i x$, R et S sont nulles, et qu'à la seconde limite $x = \pi$, on a $\sin i \pi = 0$, $R = 1$, $S = 0$, il viendra :

$$b_i = \frac{2}{\pi} \cdot \frac{i^2}{a} \int_0^\pi S \sin i x dx,$$

$$c_i = -\frac{2}{\pi} \cdot \frac{i \cos i \pi}{a} - \frac{2i^2}{\pi a} \int_0^\pi R \sin i x dx.$$

Mais d'après les équations (9) les deux intégrales précédentes sont respectivement équivalentes à $\frac{\pi}{2} b_i$, $\frac{\pi}{2} c_i$. La substitution de ces valeurs donne ces deux relations entre b_i et c_i :

$$b_i = \frac{i^2}{a} c_i, \quad c_i = -\frac{2}{\pi} \cdot \frac{i \cos i \pi}{a} - \frac{i^2}{a} b_i.$$

d'où l'on tire :

$$b_i = -\frac{2}{\pi} \cdot \frac{i^3 \cos i \pi}{a^2 + i^4}, \quad c_i = -\frac{2}{\pi} \cdot \frac{i a \cos i \pi}{a^2 + i^4}.$$

Mettant ces valeurs des coefficients b_i et c_i dans R et S (8), substituant ensuite R et S ainsi transformées dans l'expression (7) et intervertissant l'ordre des signes Σ et f , l'expression (7) deviendra :

$$(10) \quad -\frac{1}{\pi} \int_0^\pi f(\mu) d\mu \Sigma \frac{2i \cos i \pi \sin i x}{\pi} \left(\int_0^\infty \frac{i^2 \cos a(t-\mu)}{a^2 + i^4} du + \int_0^\infty \frac{a \sin a(t-\mu)}{a^2 + i^4} du \right).$$

Les deux intégrales relatives à a que renferme cette expression sont faciles à

obtenir par les formules connues. On a, comme l'on sait:

$$\int_0^{\infty} \frac{b \cos al}{b^2 + u^2} du = \frac{\pi}{2} e^{\mp bl}, \quad \int_0^{\infty} \frac{a \sin al}{a^2 + b^2} du = \pm \frac{\pi}{2} e^{\mp bl},$$

b désignant une quantité positive, et le signe supérieur ou le signe inférieur ayant lieu selon que l est positif ou négatif. En comparant ces résultats avec les intégrales précédentes, on voit que ces deux intégrales ont l'une et l'autre la valeur $\frac{\pi}{2} e^{-\sigma(t-\mu)}$ lorsque $t-\mu$ est positif, et que lorsque $t-\mu$ est négatif, elles ont respectivement les valeurs:

$$\frac{\pi}{2} e^{\sigma(t-\mu)}, \quad -\frac{\pi}{2} e^{\sigma(t-\mu)},$$

qui ne diffèrent que par les signes. Donc, la somme de ces intégrales est $\pi e^{-\sigma(t-\mu)}$ ou nulle, selon que $t-\mu$ est positif ou négatif. Il suit de là que la série contenue dans la formule (10) peut être remplacée par:

$$(11) \quad 2 \Sigma i e^{-\sigma(t-\mu)} \cos i \pi \sin i x,$$

lorsque $t-\mu$ est positif, c'est-à-dire tant que μ est inférieur à t , et qu'elle se réduit à zéro, lorsque μ surpasse t . La fonction de μ qui doit être intégrée depuis $\mu = 0$ jusqu'à $\mu = \infty$, et dont la série en question est facteur, s'évanouit donc aussi pour toutes les valeurs de μ supérieures à t .

On pourra donc n'intégrer que depuis $\mu = 0$ jusqu'à $\mu = t$; changeant ainsi la limite supérieure de l'intégrale (10) et remplaçant la série qui y entre par l'expression (11), qui lui est équivalente tant que $\mu < t$, c'est-à-dire dans toute l'étendue de l'intégration, l'expression (10) prendra cette forme très simple:

$$-\frac{2}{\pi} \int_0^t f(\mu) d\mu \Sigma i e^{-\sigma(t-\mu)} \cos i \pi \sin i x,$$

ou ce qui revient au même, en intervertissant l'ordre des signes i et Σ :

$$-\frac{2}{\pi} \Sigma i e^{-\sigma t} \cos i \pi \sin i x \int_0^t e^{\sigma \mu} f(\mu) d\mu.$$

Ayant ainsi obtenu la première partie v' de la solution, on en déduira la seconde v'' en changeant x en $\pi - x$ et $f(\mu)$ en $F(\mu)$. Si l'on ajoute ensuite v' et v'' à la troisième partie w déjà formée plus haut, on obtiendra l'expression suivante de la température variable u du point dont l'abscisse est x :

$$\begin{aligned}
 u = & -\frac{2}{\pi} \Sigma i e^{-i^2 t} \cos i \cdot \pi \sin i x \int_0^x e^{i^2 u} f(u) d\mu \\
 & -\frac{2}{\pi} \Sigma i e^{-i^2 t} \sin i x \int_0^x e^{i^2 u} F(u) d\mu \\
 & +\frac{2}{\pi} \Sigma e^{-i^2 t} \sin i x \int_0^x g(u) \sin i \mu d\mu.
 \end{aligned}$$

Cette expression diffère un peu par la forme du résultat que M. FOURIER a donné. Pour la faire coïncider avec la formule que l'on trouve dans le Mémoire déjà cité, il faut remplacer l'intégrale qui entre dans la première partie v' de u par cette expression que donne l'intégration par parties:

$$\frac{e^{i^2 t} f(t) - f(0)}{i^2} - \frac{1}{i^2} \int_0^t e^{i^2 u} f'(u) d\mu,$$

$f'(u)$ désignant la fonction dérivée de $f(u)$.

La première partie v' se change ainsi en:

$$-\frac{2}{\pi} f(t) \Sigma \frac{\cos i \pi \sin i x}{i} + \frac{2}{\pi} \Sigma e^{-i^2 t} \cos i \pi \cdot \frac{\sin i x}{i} \left(f(0) + \int_0^t e^{i^2 u} f'(u) d\mu \right).$$

Mettant maintenant à la place de $\Sigma \frac{\cos i \pi \sin i x}{i}$ sa valeur comme $-\frac{1}{2}x$, v' prendra cette forme:

$$\frac{x}{\pi} f(t) + \frac{2}{\pi} \Sigma e^{-i^2 t} \cos i \pi \frac{\sin i x}{i} \left(f(0) + \int_0^t e^{i^2 u} f'(u) d\mu \right).$$

Si l'on transforme v'' d'une manière analogue et que l'on ajoute ensuite les 3 parties v' , v'' et w , on aura l'expression de la température u , telle que M. FOURIER l'a donnée.

DÉMONSTRATION D'UNE PROPRIÉTÉ
ANALOGUE A LA LOI DE RÉCIPROCITÉ QUI
EXISTE ENTRE DEUX NOMBRES PREMIERS
QUELCONQUES.

PAR

M. G. LEJEUNE DIRICHLET,
PROF. DE MATH.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 9 p. 379—389.

DÉMONSTRATION D'UNE PROPRIÉTÉ ANALOGUE A LA LOI DE RÉCIPROCITÉ QUI EXISTE ENTRE DEUX NOMBRES PREMIERS QUELCONQUES.

Dans un mémoire qui vient d'être publié dans le recueil de la Société Royale de Gottingue, M. GAUSS a étendu le domaine de l'analyse indéterminée aux expressions de la forme $t+u\sqrt{-1}$, t et u désignant des nombres entiers positifs ou négatifs. Ce grand géomètre a reconnu que les expressions de cette espèce se rapprochent entièrement par leurs propriétés des nombres entiers réels qu'elles comprennent d'ailleurs comme cas particulier. L'analogie qui existe à cet égard est telle que les énoncés des théorèmes connus relatifs aux entiers réels peuvent être transportés pour la plupart presque littéralement dans la théorie des nombres ainsi généralisée. Il n'en est pas de même des démonstrations qui paraissent présenter de nouvelles difficultés si l'on excepte les théorèmes très simples qui dérivent immédiatement des notions fondamentales. L'induction appliquée à des questions d'un ordre plus élevé, a fait connaître à M. GAUSS une proposition qui ne le cède, ni en simplicité ni en élégance, au théorème si célèbre sous le nom de loi de réciprocité. Quant à la démonstration de ce nouveau théorème, que l'illustre auteur juge sujette à de grandes difficultés, il la renvoie à un autre mémoire où elle sera exposée avec celle d'une autre proposition plus générale. Je me propose de démontrer dans ce mémoire le théorème dont il s'agit par des considérations fort simples et qui mériteront peut-être de fixer un instant l'attention parce qu'elles sont également applicables à d'autres questions*).

*) On peut, au lieu des expressions de la forme $t+u\sqrt{-1}$, considérer celles de la forme plus générale $t+u\sqrt{a}$, a étant sans diviseur carré. Les expressions de ce genre, considérées sous le même point de vue, donnent lieu à des théorèmes analogues à celui qui fait l'objet de ce mémoire et susceptibles d'une démonstration toute semblable.

J'entre en matière en énonçant quelques définitions et en démontrant plusieurs propositions préliminaires, qui se trouvent déjà pour la plupart dans le mémoire cité plus haut.

§. 1.

Une expression de la forme $g+h\sqrt{-1}$, g et h désignant des entiers réels, sans excepter zéro, sera dite un nombre entier complexe. Il résulte de là que les entiers réels sont des cas particuliers des entiers complexes. Cette définition posée, il n'est besoin d'aucune explication pour indiquer le sens que l'on doit attacher aux mots divisibilité et congruence. De même que tout nombre réel est divisible par ± 1 , tout nombre complexe doit être considéré comme contenant les facteurs ± 1 , $\pm\sqrt{-1}$. Un nombre complexe sera dit premier lorsqu'il ne peut être décomposé en deux facteurs différents l'un et l'autre de ± 1 et $\pm\sqrt{-1}$. Voyons d'après cela comment on peut reconnaître si un nombre complexe $g+h\sqrt{-1}$ est premier ou non. Pour cela nous distinguerons deux cas selon que les deux termes g , h du nombre complexe sont ou ne sont pas l'un et l'autre différents de zéro. Le second de ces deux cas semble se subdiviser: le terme subsistant pouvant être réel ou le produit de $\sqrt{-1}$ et d'un nombre réel. Mais il est facile de voir que cela revient au même, car si $h\sqrt{-1}$ est premier, h l'est pareillement et réciproquement. Or, pour qu'un nombre réel q , considéré comme complexe, soit premier, il faut d'abord qu'il le soit aussi sous le point de vue ordinaire. Mais cela ne suffit pas: il doit en outre, abstraction faite du signe, être de la forme $4n+3$; car s'il avait la forme $4n+1$ qui entraîne toujours celle-ci: e^2+d^2 , il serait décomposable dans les facteurs $c+d\sqrt{-1}$ et $c-d\sqrt{-1}$. Réciproquement, tout nombre premier réel q qui, abstraction faite du signe, est de la forme $4n+3$, doit être aussi considéré comme premier dans la théorie des nombres complexes; car si l'on avait:

$$q = (c+d\sqrt{-1})(e+f\sqrt{-1}),$$

on aurait aussi:

$$q = (c-d\sqrt{-1})(e-f\sqrt{-1})$$

et par conséquent, en multipliant:

$$q^2 = (e^2+d^2)(e^2+f^2),$$

équation impossible, q ne pouvant être diviseur de la somme de deux carrés.

Considérons, en second lieu, le cas où aucun des deux termes de l'expression $g+h\sqrt{-1}$ ne s'évanouit. Pour qu'elle représente alors un nombre premier complexe, il est nécessaire et suffisant que g^2+h^2 soit un nombre premier réel. Pour le faire voir, supposons $g+h\sqrt{-1}$ décomposable dans les deux facteurs $c+d\sqrt{-1}$ et $e+f\sqrt{-1}$, $g-h\sqrt{-1}$ sera le produit de $e-d\sqrt{-1}$ et de $e-f\sqrt{-1}$, et l'on trouve :

$$g^2+h^2 = (e^2+d^2)(e^2+f^2).$$

c'est-à-dire g^2+h^2 égal à un nombre composé. Réciproquement si g^2+h^2 est un nombre réel composé, $g+h\sqrt{-1}$ est un nombre complexe également composé. La chose est évidente lorsque g, h ont un facteur commun; si un pareil facteur n'existe pas, g^2+h^2 n'a que des diviseurs premiers réels $4n+1$. Soit $p = e^2+d^2$ un de ces diviseurs, on aura :

$$g^2 \equiv -h^2, \quad e^2 \equiv -d^2 \pmod{p}$$

et par suite, en multipliant et transposant :

$$(cg+dh)(cg-dh) \equiv 0 \pmod{p}.$$

d'où l'on conclut que $\frac{cg \pm dh}{p}$, avec le signe convenable, est entier. On a d'un autre côté :

$$p(g^2+h^2) = (cg \pm dh)^2 + (ch \mp dg)^2,$$

équation qui exige évidemment que $\frac{ch \mp dg}{p}$ soit entier en même temps que $\frac{cg \pm dh}{p}$, les signes supérieurs et inférieurs se correspondant. Cela posé, il est évident que le quotient :

$$\frac{g+h\sqrt{-1}}{c \pm d\sqrt{-1}} = \frac{cg \pm dh}{p} + \frac{ch \mp dg}{p} \sqrt{-1}$$

est un entier complexe et $g+h\sqrt{-1}$ par conséquent un nombre composé. Il est donc prouvé que, si g^2+h^2 est un nombre premier réel, $g+h\sqrt{-1}$ est un nombre premier complexe, et réciproquement.

Il résulte de cette discussion qu'il y a des nombres premiers de deux espèces différentes. Ceux de la première espèce se réduisent à un seul terme, et ne sont autre chose, abstraction faite du signe ou du facteur $\pm\sqrt{-1}$, que

des nombres premiers réels de la forme $4n+3$. Pour plus de simplicité, nous les supposons toujours débarrassés du facteur $\sqrt{-1}$.

Ceux de la seconde espèce tirent leur origine des nombres premiers réels composés de deux carrés qui, à l'exception de 2, sont tous de la forme $4n+1$. Si l'on désigne par $c+d\sqrt{-1}$ un nombre premier de cette espèce (à l'exception de $\pm(1+\sqrt{-1})$, $\pm(1-\sqrt{-1})$ qui proviennent du nombre 2), il est évident que les entiers réels c , d sont l'un pair, l'autre impair. Cela posé, nous considérerons, pour plus d'uniformité, dans ce qui va suivre, d comme pair, ce qui est permis, car si d est impair, on n'a qu'à multiplier par $\sqrt{-1}$, ce qui donne le nombre $-d+c\sqrt{-1}$, qui est également premier et tellement lié au précédent que la connaissance des propriétés de l'un suffit pour juger de celles de l'autre.

Nous terminons ces préliminaires par la démonstration d'un théorème, dont nous aurons besoin dans la suite. Les termes réels A et B du nombre complexe $A+B\sqrt{-1}$ étant supposés premiers entre eux (ce qui exclut le cas où l'un d'eux serait nul) et $g+h\sqrt{-1}$ étant un nombre complexe quelconque, je dis qu'il existe toujours un nombre s entier réel et tel qu'on ait :

$$s \equiv g+h\sqrt{-1} \pmod{A+B\sqrt{-1}}.$$

En effet, la congruence en question revient à cette équation :

$$s-g-h\sqrt{-1} = (g+\psi\sqrt{-1})(A+B\sqrt{-1})$$

ou à celles-ci :

$$s-g = A\psi - B\psi, \quad -h = A\psi + B\psi.$$

La dernière est évidemment possible, A et B n'ayant pas de diviseur commun, et il est également manifeste que la première donnera ensuite une valeur entière pour s .

§. 2.

Ces préliminaires posés, nous arrivons au véritable objet de ce mémoire, qui est de considérer les nombres complexes, en tant qu'ils sont ou ne sont pas résidus quadratiques les uns des autres. D'après la définition connue on dit que le nombre $\alpha+\beta\sqrt{-1}$ est ou n'est pas résidu quadratique de $A+B\sqrt{-1}$, selon qu'il existe ou qu'il n'existe pas d'expression $x+y\sqrt{-1}$, telle que $(x+y\sqrt{-1})^2 - \alpha - \beta\sqrt{-1}$ soit divisible par $A+B\sqrt{-1}$. Pour décider si un

nombre complexe est ou n'est pas résidu quadratique d'un nombre complexe composé, il suffit, comme lorsqu'il s'agit de nombres réels, de considérer les différents facteurs simples du diviseur. Nous supposons donc, dans ce qui va suivre, que le diviseur ou module $A + B\sqrt{-1}$ est un nombre premier. Pour commencer par le cas le plus simple, considérons un nombre premier q de première espèce, et proposons-nous de déterminer si $\alpha + \beta\sqrt{-1}$, expression que nous supposons non-divisible par q et dans laquelle β peut être nul, est ou n'est pas résidu quadratique de q . Attribuant dans l'expression $t + u\sqrt{-1}$, à chacune des lettres t et u , les valeurs $0, 1, 2, 3, \dots, q-1$, et excluant la combinaison $0, 0$, on aura $q^2 - 1$ nombres dont nous désignerons l'ensemble par (k) . Cela posé, distinguons deux cas, selon que $\alpha + \beta\sqrt{-1}$ est ou n'est pas résidu*) de q , et commençons par l'examen du dernier. L'ensemble (k) peut être partagé, dans ce cas, en groupes composés chacun de deux nombres tels que leur produit soit $\equiv \alpha + \beta\sqrt{-1} \pmod{q}$. En effet, soit $r + s\sqrt{-1}$ l'un quelconque des nombres (k) et $r' + s'\sqrt{-1}$ celui qui doit former un groupe avec lui. Il faut donc qu'on ait :

$$(r + s\sqrt{-1})(r' + s'\sqrt{-1}) \equiv \alpha + \beta\sqrt{-1} \pmod{q},$$

c'est-à-dire :

$$rr' - ss' \equiv \alpha, \quad rs' + sr' \equiv \beta \pmod{q}.$$

On peut remplacer ces congruences par celles-ci :

$$(r^2 + s^2)r' \equiv \alpha r + \beta s, \quad (r^2 + s^2)s' \equiv \beta r - \alpha s \pmod{q}.$$

Comme $r^2 + s^2$ ne peut être divisible par q , qui est un nombre premier $4n + 3$, ces congruences sont possibles et leur résolution donnera pour r' et s' un système unique de valeurs positives et moindres que q . Il est évident d'ailleurs, par ce qu'on a supposé, qu'on ne saurait avoir à la fois $r' = 0, s' = 0$, ni $r' = r, s' = s$, ce qui suffit pour montrer la possibilité de distribuer la suite (k) en groupes tels que nous les avons définis. Or ces groupes dont chacun est composé de deux nombres tels que leur produit soit $\equiv \alpha + \beta\sqrt{-1} \pmod{q}$, étant évidemment au nombre de $\frac{1}{2}(q^2 - 1)$, il s'ensuit que le produit des nombres (k) , que nous désignerons par K , satisfait à la congruence :

$$(\alpha + \beta\sqrt{-1})^{\frac{1}{2}(q^2 - 1)} \equiv K \pmod{q}.$$

*) Comme les résidus quadratiques ou du second degré sont les seuls dont il soit question dans ce mémoire, nous supprimerons, pour abrégé, le mot quadratique.

Venons maintenant au cas où $\alpha + \beta\sqrt{-1}$ est résidu de q . Il existe alors dans la suite (k) deux nombres tels que le carré de chacun d'eux soit $\equiv \alpha + \beta\sqrt{-1} \pmod{q}$. Si l'on désigne l'un d'eux par $r + s\sqrt{-1}$, l'autre sera $q - r + (q - s)\sqrt{-1}$. Ayant ôté ces deux nombres de la suite (k) , les nombres restants pourront se partager en groupes, d'où l'on conclut que leur produit est $\equiv (\alpha + \beta\sqrt{-1})^{\frac{1}{2}(q^2-3)} \pmod{q}$. Comme on a, d'un autre côté:

$$(r + s\sqrt{-1})(q - r + (q - s)\sqrt{-1}) \equiv -(r + s\sqrt{-1})^2 \equiv -(\alpha + \beta\sqrt{-1}) \pmod{q},$$

il viendra en multipliant:

$$(\alpha + \beta\sqrt{-1})^{\frac{1}{2}(q^2-1)} \equiv -K \pmod{q}.$$

Les deux cas que nous venons de considérer, sont compris dans cet énoncé:

„On a:

$$(\alpha + \beta\sqrt{-1})^{\frac{1}{2}(q^2-1)} \equiv \mp K \pmod{q},$$

le signe supérieur ou inférieur ayant lieu selon que $\alpha + \beta\sqrt{-1}$ est ou n'est pas résidu de q ."

Le signe supérieur devant évidemment être choisi lorsque $\alpha = 1$, $\beta = 0$, il s'ensuit qu'on a:

$$K \equiv -1 \pmod{q},$$

ce qui est analogue au théorème de WILSON. On peut, d'après cela, remplacer K par -1 dans l'avant-dernière congruence ce qui donne cet énoncé très simple:

I. „On a:

$$(\alpha + \beta\sqrt{-1})^{\frac{1}{2}(q^2-1)} \equiv +1 \text{ ou } (\alpha + \beta\sqrt{-1})^{\frac{1}{2}(q^2-1)} \equiv -1 \pmod{q}$$

selon que $\alpha + \beta\sqrt{-1}$ est ou n'est pas résidu de q ."

Si l'on désigne par $\alpha' + \beta'\sqrt{-1}$ une seconde expression non-divisible par q , on conclut immédiatement de ce théorème que le produit:

$$(\alpha + \beta\sqrt{-1})(\alpha' + \beta'\sqrt{-1})$$

est résidu de q , lorsque chacun de ses deux facteurs est résidu ou non-résidu, et qu'au contraire, ce produit est non-résidu, lorsque ses facteurs sont l'un résidu, l'autre non-résidu de q . En étendant ce résultat à un plus grand nombre de facteurs, on trouve cette proposition:

II. „Le produit d'un nombre quelconque de facteurs est ou n'est pas résidu du nombre premier q , selon que parmi ces facteurs il y a un nombre pair ou impair de non-résidus de q ."

Ce théorème a également lieu pour les nombres premiers de seconde espèce, comme on le verra plus loin.

Il y a un théorème plus simple que le théorème I et qui remplit le même objet. Pour l'établir, considérons successivement les deux cas où $\alpha + \beta\sqrt{-1}$ est et où ce nombre n'est pas résidu de q . Dans le premier de ces cas, on a :

$$\alpha + \beta\sqrt{-1} \equiv (t + u\sqrt{-1})^2 \pmod{q}$$

et par conséquent aussi :

$$\alpha - \beta\sqrt{-1} \equiv (t - u\sqrt{-1})^2 \pmod{q}$$

d'où l'on conclut en multipliant et en élevant ensuite à la puissance $\frac{1}{2}(q-1)$:

$$(\alpha^2 + \beta^2)^{\frac{1}{2}(q-1)} \equiv (t^2 + u^2)^{q-1} \equiv 1 \pmod{q}$$

ou ce qui revient au même, en se servant du signe très commode employé par M. LEGENDRE :

$$\left(\frac{\alpha^2 + \beta^2}{q}\right) = 1.$$

Supposons en second lieu que $\alpha + \beta\sqrt{-1}$ soit non-résidu de q . On prendra alors deux nombres (réels) α' et β' tels que $\alpha'^2 + \beta'^2 + 1$ soit divisible par q . (L'existence de pareils nombres résulte d'un théorème connu d'EULER. *Théorie des nombres*. 3^{ième} édit. vol. I. pag. 213.)

Cela posé, on aura :

$$\alpha'^2 + \beta'^2 \equiv -1 \pmod{q},$$

et par conséquent :

$$\left(\frac{\alpha'^2 + \beta'^2}{q}\right) = -1.$$

On conclut de là que $\alpha' + \beta'\sqrt{-1}$ est non-résidu de q ; car pour qu'il fût résidu, il faudrait, d'après ce qu'on a vu dans le premier cas, qu'on eût :

$$\left(\frac{\alpha'^2 + \beta'^2}{q}\right) = 1.$$

Le produit :

$$(\alpha + \beta\sqrt{-1})(\alpha' + \beta'\sqrt{-1}) = \alpha\alpha' - \beta\beta' + (\alpha\beta' + \beta\alpha')\sqrt{-1}$$

sera donc résidu, et l'on aura :

$$\left(\frac{(\alpha\alpha' - \beta\beta')^2 + (\alpha\beta' + \beta\alpha')^2}{q}\right) = 1.$$

Or cette expression pouvant être mise sous la forme:

$$\left(\frac{\alpha^2 + \beta^2}{q}\right) \left(\frac{\alpha'^2 + \beta'^2}{q}\right) = 1,$$

on en conclut, en faisant attention à l'équation:

$$\left(\frac{\alpha'^2 + \beta'^2}{q}\right) = -1.$$

qu'on a:

$$\left(\frac{\alpha^2 + \beta^2}{q}\right) = -1.$$

Les deux résultats que nous venons d'obtenir, peuvent se réunir dans cet énoncé:

III. L'expression $\alpha + \beta\sqrt{-1}$, qui est supposée n'être pas divisible par le nombre premier q (de première espèce), est ou n'est pas résidu de q , selon que l'on a:

$$\left(\frac{\alpha^2 + \beta^2}{q}\right) = +1 \quad \text{ou} \quad \left(\frac{\alpha^2 + \beta^2}{q}\right) = -1.$$

Il résulte de là comme corollaire, en faisant successivement $\beta = 0$, $\alpha = 0$, que tout nombre réel α est résidu de q , et qu'il en est de même de toute expression imaginaire de la forme $\beta\sqrt{-1}$.

§. 3.

Nous passons aux modules qui sont des nombres premiers de seconde espèce. Désignons par $A + B\sqrt{-1}$ un pareil nombre (B étant pair), par $\alpha + \beta\sqrt{-1}$ un nombre quelconque non-divisible par $A + B\sqrt{-1}$, et faisons pour abrégé:

$$A^2 + B^2 = P,$$

P désignant un nombre premier réel $4n+1$.

Comme d'après la définition même du résidu quadratique, $\alpha + \beta\sqrt{-1}$ est dit résidu ou non-résidu de $A + B\sqrt{-1}$, selon qu'il existe ou qu'il n'existe pas d'expression $t + u\sqrt{-1}$ telle que:

$$(t + u\sqrt{-1})^2 \equiv \alpha + \beta\sqrt{-1} \pmod{A + B\sqrt{-1}},$$

et comme, d'un autre côté, on peut toujours trouver un nombre réel s qui satisfasse à la congruence:

$$s \equiv t + u\sqrt{-1} \pmod{A + B\sqrt{-1}},$$

on voit que, pour décider si $\alpha + \beta\sqrt{-1}$ est ou n'est pas résidu de $A + B\sqrt{-1}$,

tout se réduit à savoir si la congruence:

$$s^2 \equiv \alpha + \beta\sqrt{-1} \pmod{A + B\sqrt{-1}},$$

admet ou n'admet pas de solution. Pour voir de quoi dépend sa possibilité, remplaçons-la par cette équation équivalente:

$$s^2 - \alpha - \beta\sqrt{-1} = (A + B\sqrt{-1})(g + \psi\sqrt{-1}),$$

ou ce qui revient au même, par celles-ci:

$$s^2 - \alpha = Ag - B\psi, \quad -\beta = A\psi + Bg.$$

Multipliant ces dernières par A et B et ajoutant, il viendra:

$$As^2 - A\alpha - B\beta = Pg$$

d'où l'on conclut:

$$\left(\frac{A\alpha + B\beta}{P}\right) = \left(\frac{A}{P}\right).$$

On peut démontrer réciproquement que, si la condition:

$$\left(\frac{A\alpha + B\beta}{P}\right) = \left(\frac{A}{P}\right)$$

a lieu, $\alpha + \beta\sqrt{-1}$ est nécessairement résidu de $A + B\sqrt{-1}$. En effet, il est facile de voir que la condition supposée entraîne cette équation:

$$As^2 - A\alpha - B\beta = Pg = (A^2 + B^2)g^*.$$

Or cette équation pouvant être mise sous la forme:

$$A(s^2 - Ag - \alpha) = B(Bg + \beta),$$

et les nombres A, B n'ayant pas de diviseur commun, il faut que $Bg + \beta$ soit divisible par A . Faisons donc:

$$Bg + \beta = -A\psi.$$

Mettant ensuite cette expression dans la dernière équation, il viendra:

$$s^2 - \alpha = Ag - B\psi.$$

On voit par là que les deux équations nécessaires et suffisantes pour que $\alpha + \beta\sqrt{-1}$ soit résidu de $A + B\sqrt{-1}$, résultent de la condition:

$$\left(\frac{A\alpha + B\beta}{P}\right) = \left(\frac{A}{P}\right).$$

Ayant ainsi prouvé que, si $\alpha + \beta\sqrt{-1}$ est résidu de $A + B\sqrt{-1}$, on a:

$$\left(\frac{A\alpha + B\beta}{P}\right) = \left(\frac{A}{P}\right).$$

*) *Théorie des nombres* vol. I. pag. 240.

et que la réciproque a également lieu, nous pouvons en conclure que l'on a :

$$\left(\frac{A\alpha+B\beta}{P}\right) = +\left(\frac{A}{P}\right) \quad \text{ou} \quad \left(\frac{A\alpha+B\beta}{P}\right) = -\left(\frac{A}{P}\right)$$

selon que $\alpha+\beta\sqrt{-1}$ est ou n'est pas résidu de $A+B\sqrt{-1}$.

Ce résultat peut se simplifier, si l'on remarque que l'on a toujours :

$$\left(\frac{A}{P}\right) = 1.$$

Pour s'en convaincre, on considérera l'équation :

$$P = A^2+B^2,$$

et l'on décomposera A en ses facteurs simples, en posant :

$$A = g \cdot g' \cdot g'' \dots$$

les lettres g, g', g'', \dots désignant des nombres premiers réels impairs, positifs ou négatifs. Il résulte immédiatement de l'équation précédente qu'on a :

$$\left(\frac{P}{g}\right) = 1,$$

d'où l'on conclut, en appliquant un théorème connu et en se rappelant que P est de la forme $4n+1$:

$$\left(\frac{g}{P}\right) = 1.$$

On a pareillement :

$$\left(\frac{g'}{P}\right) = 1, \quad \left(\frac{g''}{P}\right) = 1, \quad \dots$$

et l'on tire de là en multipliant :

$$\left(\frac{g \cdot g' \cdot g'' \dots}{P}\right) = \left(\frac{A}{P}\right) = 1,$$

ce qu'il s'agissait de prouver. En profitant de cette remarque, on peut modifier le résultat obtenu plus haut comme il suit :

IV. „Le nombre $\alpha+\beta\sqrt{-1}$ étant supposé n'être pas divisible par le nombre premier de seconde espèce $A+B\sqrt{-1}$, si l'on pose :

$$A^2+B^2 = P,$$

je dis que $\alpha+\beta\sqrt{-1}$ sera ou ne sera pas résidu de $A+B\sqrt{-1}$, selon que l'on a :

$$\left(\frac{A\alpha+B\beta}{P}\right) = +1 \quad \text{ou} \quad \left(\frac{A\alpha+B\beta}{P}\right) = -1.$$

Si l'on pose:

$$\left(\frac{A\alpha+B\beta}{P}\right) = \varepsilon, \quad \left(\frac{A\alpha'+B\beta'}{P}\right) = \varepsilon'.$$

ε sera d'après ce théorème $+1$ ou -1 , selon que $\alpha+\beta\sqrt{-1}$ est ou n'est pas résidu de $A+B\sqrt{-1}$, et ε' aura la même signification par rapport à $\alpha'+\beta'\sqrt{-1}$. Multipliant ces expressions entre elles, remplaçant B^2 par $P-A^2$ et faisant attention qu'on a:

$$\left(\frac{A}{P}\right) = 1.$$

il viendra:

$$\varepsilon\varepsilon' = \left(\frac{A(\alpha\alpha'-\beta\beta')+B(\alpha\beta'+\beta\alpha')}{P}\right).$$

Or cette dernière expression correspondant au produit:

$$(\alpha+\beta\sqrt{-1})(\alpha'+\beta'\sqrt{-1}) = \alpha\alpha'-\beta\beta'+(\alpha\beta'+\beta\alpha')\sqrt{-1},$$

on voit facilement que le théorème II subsiste également pour les nombres premiers de seconde espèce.

§. 4.

Après avoir fixé, dans ce qui précède, les conditions qui doivent avoir lieu pour qu'un nombre complexe soit ou ne soit pas résidu quadratique d'un nombre premier quelconque, nous allons faire voir comment on peut en déduire l'expression la plus simple des caractères distinctifs des nombres premiers dont un nombre complexe donné est résidu. Mais auparavant nous ferons remarquer qu'il est permis de se borner au cas où le nombre donné est premier: car s'il est composé, il résulte du théorème II démontré plus haut que sa relation à un nombre premier quelconque, dépend de celles de ses facteurs simples à ce même nombre premier.

Nous commençons par le nombre premier $1+\sqrt{-1}$. D'après le théorème III, ce nombre sera ou ne sera pas résidu d'un nombre premier de première espèce q , selon que l'on a:

$$\left(\frac{2}{q}\right) = 1 \quad \text{ou} \quad \left(\frac{2}{q}\right) = -1.$$

On sait d'un autre côté que le premier ou le second de ces cas aura lieu, selon que q , pris positivement, a la forme $8n+7$ ou celle-ci: $8n+3$. Donc $1+\sqrt{-1}$

sera résidu de tout nombre premier de la forme $8n+7$, non-résidu au contraire des nombres premiers de la forme $8n+3$. Passons aux nombres premiers de seconde espèce. Pour décider si $1+\sqrt{-1}$ est ou n'est pas résidu d'un pareil nombre $A+B\sqrt{-1}$, il suffit, d'après le théorème IV, de savoir si l'on a :

$$\left(\frac{A+B}{P}\right) = +1 \quad \text{ou} \quad \left(\frac{A+B}{P}\right) = -1,$$

où l'on a fait, comme plus haut :

$$P = A^2 + B^2.$$

Multipliant par 2 les deux membres de cette équation, il viendra celle-ci :

$$2P = (A+B)^2 + (A-B)^2.$$

Décomposons le nombre impair $A+B$ en facteurs simples positifs ou négatifs g, g', g'', \dots de sorte que :

$$A+B = g.g'.g''\dots$$

On aura évidemment :

$$\left(\frac{2}{g}\right) = \left(\frac{P}{g}\right)$$

et par suite, en vertu de la loi de réciprocité :

$$\left(\frac{2}{g}\right) = \left(\frac{g}{P}\right).$$

D'un autre côté, il résulte d'un théorème connu que le premier membre est $+1$ ou -1 , selon que g a la forme $8n\pm 1$ ou celle-ci : $8n\pm 3$. On a pareillement :

$$\left(\frac{2}{g'}\right) = \left(\frac{g'}{P}\right), \quad \left(\frac{2}{g''}\right) = \left(\frac{g''}{P}\right), \quad \dots$$

Faisant le produit, on obtient l'équation :

$$\left(\frac{g.g'.g''\dots}{P}\right) = \left(\frac{A+B}{P}\right) = \pm 1,$$

où le signe supérieur ou inférieur doit être pris selon que parmi les facteurs g, g', g'', \dots il y en a un nombre pair ou impair de la forme $8n\pm 3$. Or il est évident que le produit :

$$A+B = g.g'.g''\dots$$

aura la forme $8n\pm 1$ ou celle-ci : $8n\pm 3$, selon que ce nombre est pair ou impair. De là et de ce qu'on a vu plus haut, résulte ce théorème :

“ $1+\sqrt{-1}$ est résidu ou non-résidu quadratique du nombre premier $A+B\sqrt{-1}$ selon que l'on a $A+B \equiv \pm 1$ ou $A+B \equiv \pm 3 \pmod{8}$.”

On peut remarquer que cet énoncé comprend ce que nous avons trouvé plus haut sur la relation de $1 + \sqrt{-1}$ aux nombres premiers de première espèce. Quant à la relation de $1 - \sqrt{-1}$ aux différents nombres premiers, elle se déduit immédiatement du théorème précédent.

Après avoir terminé ce qui regarde le nombre $1 \pm \sqrt{-1}$, nous allons nous occuper des autres nombres premiers. Désignons par $\alpha + \beta\sqrt{-1}$ un nombre premier de seconde espèce (β étant pair) et par $A + B\sqrt{-1}$ un autre nombre premier de la même espèce (B étant également pair), et proposons-nous de fixer la relation que le premier a au second.

Cette relation se détermine par un théorème très simple et qui consiste en ce que le premier est ou n'est pas résidu du second, selon que le second est ou n'est pas résidu du premier. Pour démontrer ce théorème, faisons pour abrégé :

$$\alpha^2 + \beta^2 = p, \quad A^2 + B^2 = P.$$

Il résulte du théorème IV que $\alpha + \beta\sqrt{-1}$ est ou n'est pas résidu de $A + B\sqrt{-1}$, selon que l'on a :

$$\left(\frac{A\alpha + B\beta}{P} \right) = +1 \quad \text{ou} \quad \left(\frac{A\alpha + B\beta}{P} \right) = -1.$$

En échangeant les nombres $\alpha + \beta\sqrt{-1}$ et $A + B\sqrt{-1}$ entre eux, ce qui ne change pas l'expression $A\alpha + B\beta$, on conclut de la même proposition que $A + B\sqrt{-1}$ est ou n'est pas résidu de $\alpha + \beta\sqrt{-1}$, selon que l'on a :

$$\left(\frac{A\alpha + B\beta}{p} \right) = +1 \quad \text{ou} \quad \left(\frac{A\alpha + B\beta}{p} \right) = -1.$$

On voit par là que la démonstration du théorème énoncé plus haut se réduit à faire voir que l'équation :

$$\left(\frac{A\alpha + B\beta}{P} \right) = \left(\frac{A\alpha + B\beta}{p} \right)$$

a toujours lieu. Pour cela on fait le produit de p et de P , on trouve ainsi :

$$(A\alpha + B\beta)^2 + (A\beta - B\alpha)^2 = pP.$$

Comme, par hypothèse, A et α sont impairs, B et β pairs, $A\alpha + B\beta$ sera un nombre impair. Désignant par g, g', g'', \dots ses facteurs simples, on a :

$$A\alpha + B\beta = g \cdot g' \cdot g'' \dots$$

et l'équation précédente donne immédiatement :

$$\left(\frac{p}{g} \right) = \left(\frac{P}{g} \right).$$

d'où l'on conclut, en vertu d'un théorème connu :

$$\left(\frac{g}{p}\right) = \left(\frac{g}{P}\right).$$

On a pareillement :

$$\left(\frac{g'}{p}\right) = \left(\frac{g'}{P}\right), \quad \left(\frac{g''}{p}\right) = \left(\frac{g''}{P}\right), \quad \dots,$$

d'où l'on tire en multipliant :

$$\left(\frac{g \cdot g' \cdot g'' \dots}{p}\right) = \left(\frac{g \cdot g' \cdot g'' \dots}{P}\right) \quad \text{ou} \quad \left(\frac{A\alpha + B\beta}{p}\right) = \left(\frac{A\alpha + B\beta}{P}\right),$$

ce qu'il s'agissait de prouver.

Il existe une réciprocité analogue, lorsque les deux nombres premiers n'appartiennent pas l'un et l'autre à la seconde espèce. Pour le faire voir, soient q et $A + BV - 1$ deux nombres premiers qui sont respectivement de première et de seconde espèce. D'après le théorème III le second sera ou ne sera pas résidu du premier, selon que l'on a :

$$\left(\frac{A^2 + B^2}{q}\right) = \left(\frac{P}{q}\right) = +1 \quad \text{ou} \quad \left(\frac{A^2 + B^2}{q}\right) = \left(\frac{P}{q}\right) = -1.$$

Il résulte, d'un autre côté, du théorème IV que le premier sera ou ne sera pas résidu du second, selon que :

$$\left(\frac{qA}{P}\right) = \left(\frac{q}{P}\right) = +1 \quad \text{ou} \quad \left(\frac{qA}{P}\right) = \left(\frac{q}{P}\right) = -1.$$

Ces deux résultats combinés avec l'égalité :

$$\left(\frac{P}{q}\right) = \left(\frac{q}{P}\right)$$

qui dérive d'un théorème connu, suffisent pour établir la réciprocité énoncée plus haut. Il ne reste plus à considérer que le cas de deux nombres premiers de première espèce. Dans ce troisième cas, la réciprocité est évidente puisque nous avons vu plus haut qu'un nombre réel quelconque est toujours résidu de tout nombre premier de première espèce. Les trois cas que nous venons d'examiner conduisant au même résultat, nous pouvons énoncer le théorème suivant qui est celui dont il a été question dans le préambule de ce mémoire.

« Désignant par $\alpha + \beta V - 1$ et $A + BV - 1$ (β et B étant pairs et pouvant se réduire à zéro) deux nombres premiers complexes, le premier sera ou ne sera pas résidu quadratique du second, selon que le second est ou n'est pas résidu quadratique du premier. »

Berlin, au mois de septembre 1832.

DÉMONSTRATION DU THÉORÈME DE FERMAT
POUR LE CAS DES 14^{IÈMES} PUISSANCES.

PAR

M. G. LEJEUNE DIRICHLET,
PROF. DE MATH. A BERLIN.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 9 p. 390—393.

DÉMONSTRATION DU THÉORÈME DE FERMAT POUR LE CAS DES 14^{ÈMES} PUISSANCES.

Si l'existe des nombres entiers t , u , v propres à satisfaire à l'équation:

$$(1) \quad t^{14} = u^{14} + v^{14},$$

il est manifeste que tout facteur commun δ de deux d'entre eux, divisera nécessairement aussi le troisième. On pourra donc diviser chacun d'eux par δ , ce qui ne changera en rien la forme de l'équation: d'où l'on conclut, qu'il est permis, pour prouver l'impossibilité de l'équation (1), d'y considérer les entiers t , u , v , pris deux à deux, comme libres de tout facteur commun. Cela posé, ces entiers devront évidemment être supposés l'un pair, les autres impairs, et le nombre pair sera l'un de ceux que renferme le second membre. On voit aussi que si parmi ces nombres il y en a un divisible par 7, ce ne saurait être t , puisque 7 ne peut jamais diviser la somme de deux carrés premiers entre eux. L'équation étant symétrique par rapport à u et à v , nous pourrions supposer que, si parmi ces nombres il y a un multiple de 7, v se trouve dans ce cas. Transposant le terme en u , l'équation se changera en celle-ci:

$$(2) \quad t^{14} - u^{14} = v^{14}$$

qu'on peut mettre sous cette autre forme:

$$(3) \quad (t^2 - u^2)[(t^2 - u^2)^6 + 7t^2u^2(t^4 - t^2u^2 + u^4)^2] = v^{14}.$$

Les nombres t , u ayant été supposés premiers entre eux, $t^2 - u^2$ et tu sont aussi sans diviseur commun: il en est de même de $t^2 - u^2$ et $t^4 - t^2u^2 + u^4$, car tout nombre premier diviseur commun de ceux-ci diviserait:

$$t^4 - t^2u^2 + u^4 - (t^2 - u^2)^2 = t^2u^2,$$

et par conséquent aussi tu . Les nombres tu et $t^2 - u^2$ auraient donc ce même diviseur commun, ce qui ne s'accorde pas avec ce qu'on vient de prouver. Il résulte de là, si l'on fait pour abrégier:

$$t^2 - u^2 = \varphi, \quad tu(t^4 - t^2u^2 + u^4) = \psi,$$

que g et ψ , qui sont évidemment l'un pair, l'autre impair, n'ont pas de diviseur commun, et l'on aura:

$$(4) \quad g((g^3)^2 + 7\psi^2) = r^{14}.$$

Nous distinguons maintenant deux cas, selon que r est ou n'est pas divisible par 7. Si l'on suppose en premier lieu r non-divisible par 7, g ne le sera pas non plus. Il suit de là et de ce que g et ψ sont premiers entre eux, que les deux facteurs du premier membre sont aussi premiers entre eux et par conséquent égaux l'un et l'autre à des 14^{ièmes} puissances. D'un autre côté, l'on conclut d'un théorème connu que la racine de la 14^{ième} puissance impaire $(g^3)^2 + 7\psi^2$ a la même forme, $g^2 + 7h^2$, et l'on prouve facilement*) que les entiers g , h satisfont à l'équation:

$$g^3 + \psi\sqrt{-7} = (g+h\sqrt{-7})^{14}$$

où il faut évaluer séparément les parties réelles et les coefficients de $\sqrt{-7}$. Sans développer cette expression, il est évident que la valeur qu'elle donne pour ψ est divisible par 7. Mais ψ étant égal à:

$$tu(t^4 - t^2u^2 + u^4) = tu((t^2 - u^2)^2 + t^2u^2)$$

ne peut être divisible par 7, à moins que t ou u ne le soit, ce qui serait contraire à la supposition faite plus haut. Il est donc prouvé que le cas où l'on suppose r non-divisible par 7, en même temps que t et u , ne saurait avoir lieu. Reste à faire voir que l'équation (2) ne peut pas subsister non plus, si l'on considère r comme un multiple de 7. En y faisant:

$$r = 7w$$

elle deviendra:

$$t^{14} - u^{14} = 7^{14}w^{14}.$$

C'est l'équation dont il s'agit de prouver l'impossibilité. Sans compliquer la marche de la démonstration, nous pouvons, au lieu de l'équation précédente, traiter l'équation plus générale:

$$(5) \quad t^{14} - u^{14} = 2^n 7^{1+n} w^{14}$$

*) Pour prouver ce dont il s'agit, on peut s'y prendre à peu près de la même manière dont nous avons démontré un théorème analogue (Voi. III de ce Journal, page 359, 360). Les théorèmes I (page 355) et III (page 358) ainsi que leurs démonstrations subsistent également, lorsque a est négatif. Supposant donc $a = -7$, la démonstration s'achève comme à l'endroit cité; elle est même plus simple en ce qu'elle n'est pas compliquée de la considération des solutions, en nombre infini, de l'équation $t^2 - au^2 = 1$ qui n'en a qu'une lorsque a est négatif.)

2) Von den citirten Stellen findet sich die erste auf S. 28, 29, die zweite auf S. 24, die dritte auf S. 27 dieser Ausgabe von G. Lejeune Dirichlet's Werke.

les nombres t, u étant toujours supposés sans diviseur commun, et m, n désignant des entiers positifs (sans excepter zéro).

En conservant toutes les dénominations précédentes, l'équation pourra être mise sous cette forme:

$$g((g^3)^2 + 7\psi^2) = 2^m 7^{1+n} r^{14}.$$

Comme elle exige évidemment que g soit divisible par 7, faisons $g = 7\chi$; nous aurons ainsi:

$$7^2 \chi(\psi^2 + 7(7^2 \chi^3)^2) = 2^m 7^{1+n} r^{14}.$$

Il est facile de voir que les deux facteurs $7^2 \chi$ et $\psi^2 + 7(7^2 \chi^3)^2$, dont le second est impair, n'ont pas de diviseur commun. Il résulte de là que l'équation précédente ne peut subsister à moins que $\psi^2 + 7(7^2 \chi^3)^2$ et $7^2 \chi$ ne soient le premier une 14^{ième} puissance, le second le produit d'une pareille puissance par $2^m 7^{1+n}$. Quant à la première de ces conditions, elle exige, d'après ce qu'on a vu plus haut, qu'on ait:

$$\psi + 7^2 \chi^3 \sqrt{-7} = (r+s\sqrt{-7})^{14},$$

c'est-à-dire:

$$7^2 \chi^3 = \frac{(r+s\sqrt{-7})^{14} - (r-s\sqrt{-7})^{14}}{2\sqrt{-7}},$$

où les entiers r, s sont premiers entre eux, l'un pair, l'autre impair et le premier de plus non-divisible par 7. On peut faire subir à cette expression une transformation semblable à celle que nous avons effectuée sur le premier membre de l'équation (2). Il suffit pour cela de remplacer dans le premier membre de l'équation (3), t et u respectivement par $r+s\sqrt{-7}$ et $r-s\sqrt{-7}$. En opérant ainsi et en faisant pour abrégér:

$$(r^2 + 7s^2)(r^4 - 2 \cdot 7^2 r^2 s^2 + 7^2 s^4) = R,$$

on obtient:

$$7^2 \chi^3 = 2 \cdot 7 \cdot rs [R^2 - (7 \cdot 4^3 r^3 s^3)^2]$$

ou, ce qui revient au même, en multipliant les deux membres par 7^4 :

$$7^6 \chi^3 = 2 \cdot 7^5 rs (R + 7(4rs)^3)(R - 7(4rs)^3).$$

Il est facile de faire voir que les trois facteurs $2 \cdot 7^5 rs$, $R + 7(4rs)^3$, $R - 7(4rs)^3$, pris deux à deux, n'ont pas de diviseur commun. Il est d'abord évident que s'il y a un diviseur commun, ce ne peut être ni 2 ni 7, car les deux derniers des nombres en question sont impairs et non-divisibles par 7. Soit en second lieu p un nombre premier impair différent de 7, et supposons qu'il soit divi-

seur commun de deux des expressions dont il s'agit. On s'aperçoit, à leur seule inspection, que p sera facteur commun de rs et R , et en faisant ensuite attention à la manière dont l'expression R est composée en r et s , il est évident qu'il est nécessaire que p divise à la fois r et s , ce qui est absurde, r et s étant premiers entre eux. Nous avons vu plus haut que $7^2\chi$ devait être une 14^{ième} puissance multipliée par $2^m 7^{1+n}$; le premier membre $7^6\chi^3$ de la dernière équation sera donc le produit d'une puissance du même degré et de $2^{3m} 7^{3+3n}$. Il résulte de là et de ce que les trois facteurs du second membre sont premiers entre eux, que les deux derniers sont des 14^{èmes} puissances, et que le premier est le produit d'une pareille puissance et de $2^{3m} 7^{3+3n}$. On aura donc :

$$2 \cdot 7^3 rs = 2^{3m} 7^{3+3n} e^{14}, \quad R + 7(4rs)^3 = r^{14}, \quad R - 7(4rs)^3 = u^{14}.$$

Il est facile de voir qu'on peut mettre le second membre de la première de ces équations sous la forme $2^{3m} 7^{6+n'} e'^{14}$, où n' désigne un entier positif ou zéro. Lorsque n diffère de zéro, la chose est évidente; dans le cas où $n = 0$, il faut, pour que le second membre puisse être égal au premier membre, qui est divisible par 7^5 , que r' soit un multiple de 7. Mettant en conséquence $7v'$ à la place de r' , le second membre prendra encore la forme supposée. Nous pouvons donc remplacer la première des équations précédentes par celle-ci :

$$4rs = 2^{3m+1} 7^{1+n'} e'^{14}.$$

Prenant ensuite la différence des deux dernières, comparant et posant pour abrégier $v^3 = u'$, il viendra :

$$r^{14} - u'^{14} = 2^{3m+4} 7^{3n'+4} v'^{14}.$$

Cette équation dans laquelle t' et u' n'ont pas de diviseur commun, est entièrement semblable à l'équation (5) dont elle dérive. Seulement, les entiers t' , u' qui y entrent, sont beaucoup plus petits que leurs analogues t , u dans l'équation (5). On est en droit de conclure de là, à la manière ordinaire, que l'équation (5), et par conséquent aussi l'équation (1) ne saurait avoir lieu.

Berlin, au mois d'octobre 1832.

UNTERSUCHUNGEN ÜBER DIE THEORIE DER QUADRATISCHEN FORMEN.

VON

G. LEJEUNE DIRICHLET.

Abhandlungen der Königlich Preussischen Akademie der Wissenschaften 1833. S. 101 — 121.

UNTERSUCHUNGEN ÜBER DIE THEORIE DER QUADRATISCHEN FORMEN.

[Gelesen in der Akademie der Wissenschaften am 15. August 1833.]

Unter den von FERMAT entdeckten, ohne Beweis überlieferten Eigenschaften der Zahlen ist besonders der Zusammenhang gewisser Formen des ersten und des zweiten Grades merkwürdig, indem die darüber von ihm aufgestellten Sätze die hauptsächlichste Veranlassung zu der Ausbildung der Theorie der Zahlen geworden sind. Es scheint eine Eigenthümlichkeit dieses Theils der Mathematik zu sein, dass darin grosse Fortschritte fast immer durch die Bemühungen hervorgerufen werden, wodurch man sich von der Richtigkeit einzelner auf dem Wege der Induction gefundener Sätze zu überzeugen sucht, während in allen andern Zweigen der Analysis bedeutende Resultate eine Folge neuer Gesichtspunkte zu sein pflegen, auf welche die Erfinder weit seltner durch das Bestreben, zerstreute Sätze zu concentriren, als durch das Bedürfniss gestellt werden, welches ihnen bei der Behandlung von Fragen fühlbar wird, die den bekannten Mitteln nicht mehr zugänglich sind. In diesem Sinne ist FERMAT durch die zahlreichen von ihm gefundenen Sätze der Schöpfer der Theorie der Zahlen geworden, obgleich von seinen Beweisen fast gar nichts auf die Nachwelt gekommen ist. Die grossen Schwierigkeiten, womit die Mathematiker zu kämpfen hatten, welche die FERMAT'schen Sätze zu beweisen versuchten, haben die zuweilen geäusserte Vermuthung veranlasst, FERMAT könne sich getäuscht haben, als er wiederholt und ausdrücklich erklärte, dass er für seine Sätze höchst einfache Beweise besitze. Ohne auf eine nähere Untersuchung über den Grad der Wahrscheinlichkeit dieser Vermuthung einzugehen, möchte ich nur darauf aufmerksam machen, dass eine solche Selbsttäuschung bei einem Mathematiker von FERMAT's unbestreitbarer Tiefe in einem Jahrhundert, welches noch ganz an die Strenge gewöhnt war, die sich die Griechen in arithmetischen Untersuchungen eben so sehr als in der Geometrie zur Pflicht gemacht hatten, viel schwerer zu erklären ist als in einer spätern Zeit, wo die Leichtigkeit und Einförmigkeit der neuen analytischen Methoden die Behandlung mathematischer

Gegenstände zuweilen in einen Mechanismus ausarten liess, dem man mit der grössten Zuversicht folgte, ohne auch nur an die Möglichkeit zu denken, dass die erhaltenen Resultate irgend einer Beschränkung unterworfen sein könnten.

In jedem Falle ist es für die Wissenschaft ein Vortheil gewesen, dass FERMAT seine Sätze nicht bloss als durch Induction gefunden, sondern als mit strengen Beweisen versehen dargestellt hatte, indem es dadurch für die Mathematiker des vorigen Jahrhunderts zu einer Art von Ehrensache wurde, in diesem Punkte nicht hinter einem Vorgänger zurückzubleiben, seit dessen Auftreten alle übrigen Theile der Wissenschaft einen so grossen Aufschwung genommen hatten. EULER, welcher zuerst nach FERMAT seine Aufmerksamkeit auf die Eigenschaften der Zahlen richtete, beschäftigte sich besonders mit dem oben erwähnten Zusammenhang, welcher zwischen Formen des ersten und zweiten Grades stattfindet, und wovon der einfachste Fall in dem Satze ausgesprochen ist, dass jede Primzahl von der Form $4n+1$, d. h. welche bei der Division durch 4 die Einheit zum Reste lässt, die Summe von zwei Quadraten oder, was dasselbe ist, in der Form t^2+u^2 enthalten ist. Seinen Bemühungen verdanken wir den Beweis des angeführten schönen Satzes und der demselben hinzugefügten Bestimmung, dass jede Primzahl von der erwähnten Linearform nur auf eine Weise in zwei Quadrate zerlegt werden könne. Aehnlichen Erfolg hatten die unermüdlichen Anstrengungen dieses grossen Forschers für mehrere dem genannten verwandte FERMAT'sche Sätze, deren Anzahl er ausserdem auf dem Wege der Induction bedeutend vermehrte.

LAGRANGE, der sich bald nach EULER mit demselben Gegenstande beschäftigte, wusste der von diesem begonnenen Untersuchung einen neuen eben so einfachen als fruchtbaren Gesichtspunkt abzugewinnen, von wo aus sich bald alles zu einer umfassenden Theorie gestaltete. Das Wesen der von ihm geschaffenen Methode besteht in der Betrachtung der einfachen Divisoren der quadratischen Form t^2+cu^2 , in welcher c eine gegebene positive oder negative ganze Zahl, t und u aber unbestimmte ganze Zahlen bezeichnen. Jeder Divisor einer solchen Form ist in einer dreigliedrigen Form:

$$gt^2+2htu+ku^2$$

enthalten, deren Coefficienten g , $2h$ und k mit c in der durch die Gleichung $gk-h^2=c$ ausgedrückten Beziehung stehen*). Diese Abhängigkeit der Coef-

*) *Théorie des Nombres* no. 138. (Troisième édition.)

ficienten, wie sie sich unmittelbar aus der Voraussetzung ergibt, dass die eine Form durch die andere numerisch theilbar sei, lässt bei einem bestimmten Werthe von c unendlich viele Formen für den Divisor zu. Diese Formen aber sind nicht alle wesentlich von einander verschieden, sondern gehen durch die Einführung anderer unbestimmter Zahlen, welche an die Stelle von t und u treten, wobei der Grad ihrer Allgemeinheit ganz ungeändert bleibt, theilweise in einander über und reduciren sich solcherweise auf eine endliche Anzahl von Formen, die nicht nur nicht in einander transformirt werden können, sondern von denen auch keine eine Primzahl enthält, die durch eine der andern dargestellt werden kann. Diese Reduction der dreigliedrigen Formen oder quadratischen Divisoren auf eine endliche Anzahl wesentlich von einander verschiedener ist besonders, wenn c eine negative Zahl bedeutet, ein sehr schwieriges Problem, dessen vollständige Lösung die Anwendung einer schon früher von LAGRANGE bei einem verwandten Gegenstande gebrauchten Analyse erforderte. Eine weitere Untersuchung der reducirten quadratischen Formen zeigte, dass denselben gewisse Ausdrücke des ersten Grades entsprechen, so dass jeder in einer quadratischen Form enthaltenen Primzahl eine der entsprechenden Linearformen zukommt. Dass aber umgekehrt jede in einer der Linearformen enthaltene Primzahl eine der entsprechenden quadratischen Formen annehmen könne, geht aus dieser Betrachtungsweise nicht hervor, und es bedarf zum Beweise dieses umgekehrten Satzes der Nachweisung, dass eine solche Primzahl wirklich ein Divisor der Formel $t^2 + cu^2$ ist. Für die Primzahlen von der Form $4n+3$ liess sich die Sache ziemlich leicht erledigen, indem von solchen gezeigt wurde, dass sie immer einer der beiden Formen:

$$t^2 + cu^2, \quad t^2 - cu^2,$$

aber auch nur einer derselben, als Divisoren angehören, woraus folgt, dass man sich in diesem Falle nur zu überzeugen hat, dass eine solche Primzahl von den Linearformen für die Divisoren der einen ausgeschlossen ist, um daraus folgern zu können, dass sie der andern als Divisor angehört. Für die Primzahlen der Form $4n+1$ bot die Frage bedeutende Schwierigkeiten dar, die es LAGRANGE nur in speciellen Fällen zu beseitigen gelang. Ich führe seine eignen Worte über diesen Punkt hier an, die für die Geschichte der Wissenschaft interessant sind, weil daraus hervorgeht, dass er den umgekehrten Satz in seinem ganzen Umfang als richtig erkannt hatte, wemgleich seine Methode zu einer vollständigen Beweisführung nicht ausreichte.

„Or quoique l'induction paraisse prouver que les nombres premiers des formes qui conviennent aux diviseurs de $t^2 \pm au^2$, peuvent toujours être effectivement des diviseurs de pareils nombres, cette proposition ne peut être prouvée rigoureusement par rapport aux nombres premiers $4n+1$ que pour un très petit nombre de cas; du moins toutes les tentatives que j'ai faites pour en venir à bout ont été jusqu'à présent inutiles: de sorte que je me bornerai ici à rapporter les résultats de mes recherches dans quelques cas particuliers où j'ai réussi à trouver la démonstration de la proposition dont il s'agit.“ *)

So fehlte also der grossen Entdeckung von LAGRANGE noch ein wesentliches Moment, um die Reihe der von FERMAT aufgestellten Sätze zu vervollständigen oder vielmehr ins Unbestimmte zu verlängern.

LEGENDRE, der einige Jahre später die Untersuchungen von LAGRANGE wieder aufnahm, zeigte, dass der eben erwähnte Satz von einem andern abhängig sei, der durch seine Einfachheit und Fruchtbarkeit gleich merkwürdig seitdem unter dem Namen des Reciprocitätsgesetzes berühmt geworden ist. Aber trotz seiner Einfachheit standen doch dem Beweise desselben sehr grosse Schwierigkeiten im Wege, die LEGENDRE durch die scharfsinnigsten Betrachtungen nur theilweise zu heben vermochte, bis endlich GAUSS in seinen 1801 erschienenen „*disquisitiones arithmeticae*“ zwei Beweise desselben mittheilte. Spätere Abhandlungen dieses grossen Mathematikers enthalten noch mehrere andere, von denen namentlich zwei, die übrigens von demselben Princip ausgehen, so einfach sind, dass jetzt sogar für die Darstellung dieser Theorie wie sie für ein Elementenbuch passt, gar nichts mehr zu wünschen bleibt.

Auf diese Weise vervollständigt und in gewissem Sinne abgeschlossen, bietet die von FERMAT und EULER vorbereitete, von LAGRANGE in ihrem ganzen Umfang erkannte Theorie der quadratischen Formen und der entsprechenden Linearformen der durch sie darstellbaren Zahlen noch mehrere Fragen dar, von denen ich eine in der Abhandlung, welche ich der Akademie vorzulegen die Ehre habe, zu behandeln versuche.

Um den Gegenstand dieser Frage näher zu bezeichnen, ist es nöthig einige specielle Resultate anzugeben, welche aus der Theorie hervorgehen, deren allmähliche geschichtliche Entwicklung ich so eben angedeutet habe. Ich werde

*) Mémoires de l'Académie de Berlin, Année 1775 p. 350.

nich dabei auf den Fall beschränken, wo die vorher c genannte Zahl eine Primzahl ist, weil für diesen Fall die Frage sich in ihrer einfachsten Gestalt darstellt. Unter dieser Voraussetzung bilden die Linearformen, welche den einfachen Divisoren von $t^2 + cu^2$ zukommen, eine oder zwei Gruppen, je nachdem c mit seinem Zeichen genommen, bei der Division durch 4 die Einheit negativ oder positiv genommen, zum Reste lässt. Wenn nun im ersteren Falle diesen Linearformen oder im letzteren Falle einer oder jeder der beiden Gruppen derselben, die sich dadurch von einander unterscheiden, dass die eine nur Primzahlen der Form $4n+1$, die andere nur solche der Form $4n+3$ enthält, mehrere quadratische Formen entsprechen, so liegt in der erwähnten Theorie eine Unvollständigkeit, indem sie zwar zeigt, dass eine Primzahl, sobald sie in einer der Linearformen enthalten ist, nothwendig eine der entsprechenden quadratischen Formen annehmen könne, allein durchaus kein Mittel angiebt *a priori* zu entscheiden, welche der quadratischen Formen ihr zukommt. Lässt man sich von der Analogie leiten, so geräth man leicht auf die Vermuthung, es könne die Gesammtheit der Linearformen einer Gruppe, der mehrere quadratische Formen entsprechen, in mehrere Unterabtheilungen zerfallen, von denen jede nur einer quadratischen Form angehöre. Allein diese Vermuthung bestätigt sich nicht, denn man findet bald, dass jede quadratische Form Primzahlen von jeder einzelnen Linearform darstellt. Es erhellt hieraus, dass die charakteristischen Eigenschaften der einzelnen zu einer Gruppe gehörigen quadratischen Formen nicht durch die den Primzahlen, welche sie enthalten, zukommenden Linearformen ausgedrückt werden können, sondern nothwendig von einem andern bisher in dieser Theorie nicht vorhandenen Elemente abhängig sein müssen. Eine schon vor mehreren Jahren unternommene Untersuchung, deren Gegenstand mit der vorher aufgeworfenen Frage in gar keinem Zusammenhange zu stehen scheint, hat mich auf einige Sätze geführt, welche für einzelne Fälle die charakteristischen Eigenschaften der in den verschiedenen quadratischen Formen enthaltenen Primzahlen kennen lehren, und zugleich den Weg bezeichnen, auf welchem sich die Induction zu allgemeineren Sätzen zu erheben hat. Obgleich die von mir gefundenen Resultate sich nicht auf den Fall beschränken, wo die oben mit c bezeichnete Zahl eine Primzahl ist, so soll doch dieser Fall, als der einfachere, in dieser Abhandlung ausschliesslich betrachtet werden.*)

*) Die im Folgenden entwickelte Methode bleibt fast ohne Modification anwendbar, wenn a eine zusammengesetzte Zahl ist.

§. 1.

Wir werden uns häufig eines von LEGENDRE eingeführten Zeichens bedienen, dessen Bedeutung also vor allen Dingen festzustellen ist. Ist p eine ungerade Primzahl und k irgend eine nicht durch p theilbare Zahl, so lässt $k^{\frac{p-1}{2}}$ den Rest $+1$ oder -1 bei der Division durch p , und zwar findet das erstere oder letztere bekanntlich statt, je nachdem k quadratischer Rest oder Nichtrest von p ist. Diesen Rest ± 1 nun werden wir mit LEGENDRE durch:

$$\left(\frac{k}{p}\right)$$

bezeichnen. Es ist nach der Bedeutung dieses Zeichens klar, dass:

$$\left(\frac{k}{p}\right)\left(\frac{k}{p}\right) = 1 \quad \text{und} \quad \left(\frac{k}{p}\right)\left(\frac{l}{p}\right) = \left(\frac{kl}{p}\right)$$

ist, wo l wie k eine nicht durch p theilbare Zahl bezeichnet. Auch folgt aus bekanten Sätzen*), dass $\left(\frac{2}{p}\right) = 1$, wenn p von der Form $8n \pm 1$, dass hingegen $\left(\frac{2}{p}\right) = -1$, wenn p in der Form $8n \pm 5$ enthalten ist. Das Reciprocitätsgesetz, welches zwischen irgend zwei ungeraden Primzahlen stattfindet**), lässt sich vermittelst dieses Zeichens sehr einfach ausdrücken. Denkt man sich nämlich unter k ebenfalls eine ungerade Primzahl, so ist dasselbe in der Gleichung:

$$\left(\frac{k}{p}\right) = \pm \left(\frac{p}{k}\right)$$

enthalten, in welcher das untere Zeichen zu nehmen ist, wenn die ungeraden Primzahlen beide von der Form $4n+3$ sind, das obere Zeichen dagegen, wenn jede oder auch nur eine die Form $4n+1$ hat. Dies vorausgesetzt wenden wir uns zu den in der Einleitung angekündigten Betrachtungen.

§. 2.

Es sei a eine Primzahl der Form $8n+1$ und p, q zwei andere Primzahlen von der Form $4n+1$, von solcher Beschaffenheit, dass:

$$\left(\frac{a}{p}\right) = 1 \quad \text{und} \quad \left(\frac{a}{q}\right) = 1.$$

*) *Théorie des Nombres*, no. 150.

**) *Théorie des Nombres*, no. 166.

Die Zahl p ist vermöge dieser Bedingungen in einem der quadratischen Divisoren $4n+1$) von der Formel t^2+au^2 , und als Primzahl auch nur in einem derselben enthalten**). Dasselbe gilt von der Zahl q . Wir machen nun die neue Annahme, dass beide Primzahlen p, q durch denselben quadratischen Divisor ausgedrückt werden, woraus nach einem bekannten Satze***) folgt, dass das Product pq in der Formel t^2+au^2 selbst enthalten ist. Wir haben also folgende Gleichung:

$$(1) \quad t^2+au^2 = pq,$$

in welcher offenbar die Zahlen t, u keinen gemeinschaftlichen Factor haben. Auch ist klar, dass von diesen Zahlen die eine gerade, die andere ungerade sein wird. Wir unterscheiden jetzt zwei Fälle, je nachdem p, q , von denen jede bei der Division durch 8 den Rest 1 oder den Rest 5 lassen kann, gleiche oder verschiedene Reste geben.

Erster Fall. Die Primzahlen p und q sind entweder beide von der Form $8n+1$, oder beide von der Form $8n+5$, d. h. ihr Product pq hat die Form $8n+1$.

Wir wollen bei diesem ersten Falle zwei Unterabtheilungen eintreten lassen, je nachdem t oder u ungerade ist. Ist t ungerade, also u gerade, so setze man:

$$t = gg'g'' \dots \quad u = 2^3 h h' h'' \dots,$$

wo $g, g', g'', \dots, h, h', h'', \dots$ ungerade Primzahlen bezeichnen. Die Gleichung (1) giebt unmittelbar:

$$\left(\frac{a}{g}\right) = \left(\frac{pq}{g}\right) = \left(\frac{p}{g}\right) \left(\frac{q}{g}\right),$$

und wenn man das Reciprocitätsgesetz anwendet, indem a, p, g Primzahlen der Form $4n+1$ sind:

$$\left(\frac{g}{a}\right) = \left(\frac{g}{p}\right) \left(\frac{g}{q}\right).$$

Bildet man ähnliche Gleichungen für g', g'', \dots und multiplicirt, so erhält man:

$$\left(\frac{gg'g'' \dots}{a}\right) = \left(\frac{gg'g'' \dots}{p}\right) \left(\frac{gg'g'' \dots}{q}\right),$$

*) Wir bedienen uns zur Abkürzung dieses Ausdrucks, um einen quadratischen Divisor zu bezeichnen, der keine andern ungeraden Zahlen als solche von der Form $4n+1$ darstellt.

**) *Théorie des Nombres*, no. 234.

***) *Théorie des Nombres*, no. 233.

oder:

$$(2) \quad \left(\frac{t}{a}\right) = \left(\frac{t}{p}\right)\left(\frac{t}{q}\right).$$

Ebenso folgt aus der Gleichung (1):

$$1 = \left(\frac{pq}{h}\right) = \left(\frac{p}{h}\right)\left(\frac{q}{h}\right), \quad \text{oder} \quad \left(\frac{h}{p}\right)\left(\frac{h}{q}\right) = 1.$$

Multipliziert man diese Gleichung mit den ähnlichen für h' , h'' , ... und mit der Gleichung $\left(\frac{2^5}{p}\right)\left(\frac{2^3}{q}\right) = 1$, die aus $\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right)$ folgt, so erhält man:

$$(3) \quad \left(\frac{u}{p}\right)\left(\frac{u}{q}\right) = 1.$$

Nimmt man, um zu der andern Unterabtheilung überzugehen, t gerade, u ungerade an, und setzt:

$$t = 2^a g g' g'' \dots, \quad u = h h' h'' \dots,$$

wo g , g' , g'' , ... und h , h' , h'' , ... wieder ungerade Primzahlen bezeichnen, so erhält man leicht aus (1):

$$\left(\frac{g}{a}\right) = \left(\frac{g}{p}\right)\left(\frac{g}{q}\right)$$

und durch Multiplication dieser Gleichung mit den analogen für g' , g'' , ... und mit der aus den über a , p , q , gemachten Voraussetzungen leicht folgenden $\left(\frac{2^a}{a}\right) = \left(\frac{2^a}{p}\right)\left(\frac{2^a}{q}\right)$:

$$\left(\frac{t}{a}\right) = \left(\frac{t}{p}\right)\left(\frac{t}{q}\right).$$

was mit (2) zusammenfällt. Ebenso findet man, dass die Gleichung (3) ebenfalls stattfindet.

Zweiter Fall. Von den Primzahlen p , q hat die eine die Form $8n+1$, die andere die Form $8n+5$, d. h. pq ist von der Form $8n+5$.

Da a und jedes ungerade Quadrat von der Form $8n+1$ ist, so folgt aus der Gleichung (1), deren zweite Seite die Form $8n+5$ hat, dass das auf der ersten Seite vorkommende gerade Glied nicht durch 8 theilbar sein kann. Es ist also diejenige der Zahlen t , u , welche gerade ist, bloss durch 2, nicht aber durch 4 theilbar. Betrachten wir zunächst t als ungerade, so haben wir:

$$t = g g' g'' \dots, \quad u = 2 h h' h'' \dots,$$

wo wieder g , g' , g'' , ... , h , h' , h'' , ... ungerade Primzahlen sind. Die Glei-

chung (1) giebt wieder unmittelbar:

$$\left(\frac{a}{g}\right) = \left(\frac{pq}{g}\right) = \left(\frac{p}{g}\right)\left(\frac{q}{g}\right),$$

woraus nach dem Reciprocitätsgesetze folgt:

$$\left(\frac{g}{a}\right) = \left(\frac{g}{p}\right)\left(\frac{g}{q}\right).$$

Diese Gleichung mit den ähnlichen für g', g'', \dots geltenden multiplicirt giebt wie oben:

$$\left(\frac{t}{a}\right) = \left(\frac{t}{p}\right)\left(\frac{t}{q}\right).$$

Aehnlicherwise folgt aus (1):

$$1 = \left(\frac{pq}{h}\right) = \left(\frac{p}{h}\right)\left(\frac{q}{h}\right), \text{ oder } \left(\frac{h}{p}\right)\left(\frac{h}{q}\right) = 1,$$

woraus wieder durch Multiplication in die analogen h', h'', \dots enthaltenden Gleichungen die Relation:

$$\left(\frac{hh'h''\dots}{p}\right)\left(\frac{hh'h''\dots}{q}\right) = 1$$

hervorgeht. Berücksichtigt man nun, dass, da von den Primzahlen p und q die eine von der Form $8n+1$, die andere von der Form $8n+5$ ist, von den Ausdrücken $\left(\frac{2}{p}\right)$ und $\left(\frac{2}{q}\right)$ der eine den Werth $+1$, der andere den Werth -1 und also ihr Product $\left(\frac{2}{p}\right)\left(\frac{2}{q}\right)$ den Werth -1 hat, so folgt, wenn man abermals multiplicirt:

$$\left(\frac{u}{p}\right)\left(\frac{u}{q}\right) = -1.$$

Betrachtet man nun jetzt t als gerade und setzt:

$$t = 2gg'g''\dots, \quad u = hh'h''\dots$$

so giebt die Gleichung (1) mit Anwendung des Reciprocitätsgesetzes:

$$\left(\frac{gg'g''\dots}{a}\right) = \left(\frac{gg'g''\dots}{p}\right)\left(\frac{gg'g''\dots}{q}\right),$$

woraus unter Berücksichtigung, dass $\left(\frac{2}{a}\right) = 1$ und $\left(\frac{2}{p}\right)\left(\frac{2}{q}\right) = -1$ ist, die Gleichung:

$$\left(\frac{t}{a}\right) = -\left(\frac{t}{p}\right)\left(\frac{t}{q}\right)$$

folgt. Ebenso erhält man leicht die Relation:

$$\left(\frac{u}{p}\right)\left(\frac{u}{q}\right) = 1.$$

Fasst man das Vorhergehende zusammen, so sieht man, dass, wenn die Primzahlen p und q beide die Form $8n+1$, oder beide die Form $8n+5$ haben, die beiden Gleichungen:

$$\left(\frac{t}{a}\right) = \left(\frac{t}{p}\right)\left(\frac{t}{q}\right), \quad \left(\frac{u}{p}\right)\left(\frac{u}{q}\right) = 1$$

stattfinden, dass hingegen, wenn von diesen Zahlen die eine in der Form $8n+1$, die andere in der Form $8n+5$ enthalten ist, entweder gleichzeitig:

$$\left(\frac{t}{a}\right) = \left(\frac{t}{p}\right)\left(\frac{t}{q}\right) \quad \text{und} \quad \left(\frac{u}{p}\right)\left(\frac{u}{q}\right) = -1$$

oder gleichzeitig:

$$\left(\frac{t}{a}\right) = -\left(\frac{t}{p}\right)\left(\frac{t}{q}\right) \quad \text{und} \quad \left(\frac{u}{p}\right)\left(\frac{u}{q}\right) = +1$$

ist. Man erhält ein einfacheres Resultat, wenn man die zusammengehörigen Gleichungen in einander multiplicirt.

Es ist nämlich offenbar:

$$\left(\frac{t}{a}\right)\left(\frac{u}{p}\right)\left(\frac{u}{q}\right) = \left(\frac{t}{p}\right)\left(\frac{t}{q}\right) \quad \text{oder} \quad \left(\frac{t}{a}\right)\left(\frac{u}{p}\right)\left(\frac{u}{q}\right) = -\left(\frac{t}{p}\right)\left(\frac{t}{q}\right),$$

je nachdem p und q bei der Division durch 8 gleiche oder verschiedene Reste geben, oder in blossen Zeichen ausgedrückt:

$$(4) \quad \left(\frac{t}{a}\right)\left(\frac{u}{p}\right)\left(\frac{u}{q}\right) = (-1)^{\frac{p+q-2}{4}} \left(\frac{t}{p}\right)\left(\frac{t}{q}\right).$$

§. 3.

Kehren wir jetzt zu der Gleichung (1) zurück, so giebt dieselbe unmittelbar:

$$t^2 \equiv -au^2 \pmod{p},$$

und durch Erhebung zur Potenz $\frac{p-1}{4}$:

$$t^{\frac{p-1}{2}} \equiv (-a)^{\frac{p-1}{4}} u^{\frac{p-1}{2}} \pmod{p}.$$

Man erhält auf ganz gleiche Weise:

$$t^{\frac{q-1}{2}} \equiv (-a)^{\frac{q-1}{4}} u^{\frac{q-1}{2}} \pmod{q}.$$

Setzt man zur Abkürzung:

$$a^{\frac{p-1}{4}} \equiv \varepsilon \pmod{p},$$

wo ε den Werth $+1$ oder -1 hat, je nachdem a biquadratischer Rest oder Nichtrest von p ist, und eben so:

$$a^{\frac{q-1}{4}} \equiv \varepsilon' \pmod{q},$$

so lassen sich die beiden vorhergehenden Congruenzen mit folgenden Gleichungen vertauschen:

$$\left(\frac{t}{p}\right) = \varepsilon \left(\frac{u}{p}\right) (-1)^{\frac{p-1}{4}}, \quad \left(\frac{t}{q}\right) = \varepsilon' \left(\frac{u}{q}\right) (-1)^{\frac{q-1}{4}},$$

woraus durch Multiplication und Vergleichung mit (4) folgt:

$$(5) \quad \left(\frac{t}{a}\right) = \varepsilon \varepsilon'.$$

Auf der andern Seite erhält man auch leicht aus (1):

$$t^{\frac{a-1}{2}} \equiv p^{\frac{a-1}{4}} q^{\frac{a-1}{4}} \pmod{a}.$$

Setzt man zur Abkürzung:

$$p^{\frac{a-1}{4}} \equiv \delta \pmod{a},$$

wo wieder $\delta = +1$ oder $= -1$, je nachdem p biquadratischer Rest oder Nichtrest von a ist, und ebenso:

$$q^{\frac{a-1}{4}} \equiv \delta' \pmod{a},$$

so lässt sich die obige Congruenz in die Form:

$$\left(\frac{t}{a}\right) = \delta \delta'$$

bringen, woraus sich endlich durch Vergleichung mit (5) folgendes Resultat ergibt:

$$(6) \quad \varepsilon \varepsilon' = \delta \delta'.$$

Erinnert man sich, dass ε , ε' , δ , δ' , abgesehen vom Zeichen, der Einheit gleich sind, so sieht man gleich, dass entweder gleichzeitig:

$$\varepsilon = \delta \quad \text{und} \quad \varepsilon' = \delta',$$

oder gleichzeitig:

$$\varepsilon = -\delta \quad \text{und} \quad \varepsilon' = -\delta'$$

ist. Die Gleichung $\varepsilon = \delta$ bedeutet nach Obigem, dass entweder zugleich a biquadratischer Rest von p und p biquadratischer Rest von a ist, oder zugleich a biquadratischer Nichtrest von p und p biquadratischer Nichtrest von a ist. Nennt man ein solches Verhalten der Primzahlen p und a zu einander biquadratische Reciprocität, und das umgekehrte durch die Gleichung $\varepsilon = -\delta$ ausgedrückte Verhältniss, wenn nämlich von den beiden Primzahlen die eine biquadratischer Rest von der andern ist, während diese biquadratischer Nichtrest von jener ist, biquadratische Nichtreciprocität, so lässt sich das Resultat (6) in folgender Art aussprechen:

„Die Primzahlen p und q stehen entweder beide zu a in biquadratischer Reciprocität oder beide in biquadratischer Nichtreciprocität.“

Bedenkt man jetzt, dass nach den im §. 2 gemachten Voraussetzungen p und q irgend zwei Primzahlen $4n+1$ bezeichnen, die durch denselben quadratischen Divisor von t^2+au^2 dargestellt werden können, so ist das eben erhaltene Resultat ganz gleichbedeutend mit folgendem Satze:

„Bezeichnet a eine Primzahl der Form $8n+1$, so haben alle in demselben quadratischen Divisor $4n+1$ von t^2+au^2 enthaltenen Primzahlen entweder zu a ein biquadratisches Reciprocitätsverhältniss oder alle das entgegengesetzte Verhältniss.“

Es zerfallen also hiernach die quadratischen Divisoren $4n+1$ der Form t^2+au^2 (wo a eine Primzahl $8n+1$) in zwei Klassen, von denen die eine — wir werden sie in der Folge die erste nennen — aus lauter quadratischen Formen besteht, die nur Primzahlen darstellen, welche mit a in biquadratischer Reciprocität stehen, während die Formen der zweiten Klasse nur Primzahlen von entgegengesetzter Beschaffenheit ausdrücken.

§. 4.

Nehmen wir als Beispiel den Fall wo $a = 17$. Es giebt für diesen Fall folgende zwei quadratische Divisoren $4n+1$ *):

$$t^2+17u^2, \quad 2t^2+2tu+9u^2.$$

Jeder derselben bildet eine Klasse, und man sieht leicht, wenn man besondere Werthe für t und u setzt, z. B. in der ersten Form $t = 6$, $u = 1$ und in der zweiten $t = 1$, $u = 1$, wodurch man die Primzahlen 53 und 13 erhält, die

*) *Théorie des Nombres*, Tab. IV.

respective mit 17 in biquadratischer Reciprocität und Nichtreciprocität stehen, dass in diesem besondern Falle die erste und zweite Klasse sich respective auf die Formen $t^2 + 17n^2$ und $2t^2 + 2tu + 9n^2$ reduciren. Bemerket man zugleich, dass:

$$2(2t^2 + 2tu + 9n^2) = (2t + u)^2 + 17n^2$$

ist, d. h. dass die zweite Form. mit 2 multiplicirt, mit der ersten zusammenfällt, so kann man das Resultat einfach so aussprechen:

„Jede Primzahl von der Form $4n + 1$, welche in der Formel $t^2 + 17n^2$ aufgeht^{*)}, ist einfach oder doppelt genommen in derselben Form $t^2 + 17n^2$ enthalten, je nachdem sie zu 17 in biquadratischer Reciprocität oder Nichtreciprocität steht.“

In allen diesem Beispiel ähnlichen Fällen, wo nämlich nur zwei quadratische Divisoren $4n + 1$ vorhanden sind, die alsdann jeder eine Klasse für sich bilden, giebt der obige Satz die charakteristischen Eigenschaften der in jedem derselben enthaltenen Primzahlen.

Besteht aber eine Klasse aus zwei oder mehr Formen, so geht aus unserm Satz nicht hervor, wodurch sich die in einer jeden derselben enthaltenen Primzahlen von den Primzahlen unterscheiden, welche durch die übrigen dargestellt werden.

Ohne die Behandlung dieser gewiss sehr schwierigen Frage zu versuchen, wollen wir in den folgenden Paragraphen bloss noch einige Untersuchungen darüber anstellen, wie sich sämtliche quadratische Divisoren $4n + 1$ unter die oben festgestellten zwei Klassen vertheilen.

§. 5.

Die Gesamtheit der quadratischen Divisoren von $t^2 + an^2$ (wo a wie vorher eine Primzahl der Form $8n + 1$ bezeichnet) lässt sich am übersichtlichsten darstellen, wenn man jeden Divisor in die Form bringt:

$$2\alpha t^2 + 2\beta tu + \gamma n^2,$$

wo α, β, γ ungerade positive Zahlen sind, die der Gleichung:

$$a = 2\alpha\gamma - \beta^2$$

und ausserdem den Ungleichheiten:

$$\alpha \geq \beta \quad \text{und} \quad \gamma \geq \beta$$

^{*)} Diese doppelte Bedingung ist gleichbedeutend mit der, in einer der Linearformen $68n + 1, 9, 13, 21, 25, 33, 49, 53$ enthalten zu sein. *Théorie des Nombres*, Tab. IV.

genügen*). Alle Formen, welche diese Bedingungen erfüllen, sind wesentlich von einander verschieden und entsprechen einander vermöge der symmetrischen Art, wie diese Bedingungen a und γ enthalten, paarweise wie die folgenden:

$$2a^2 + 2\beta tu + \gamma u^2, \quad at^2 + 2\beta tu + 2\gamma u^2,$$

die wir conjugirte Divisoren nennen wollen, und die offenbar die Eigenschaft haben, dass jede durch eine von ihnen darstellbare ungerade Zahl doppelt genommen in der andern enthalten ist. Da die erste Form die ungerade Zahl γ , und die zweite a ausdrückt, und da a und γ nach der Gleichung:

$$a = 2a\gamma - \beta^2,$$

in welcher a und β^2 von der Form $8n+1$ sind, entweder beide in der Form $4n+1$ oder beide in der Form $4n+3$ enthalten sind, so sieht man, dass beiden conjugirten Divisoren entweder die Form $4n+1$ oder die Form $4n+3$ zukommt. Man kann die Frage aufwerfen, ob ein Divisor sich selbst conjugirt sein könne. Die Bedingungen für die Existenz eines solchen Divisors bestehen nach Obigem darin, dass sowohl $a = 2a^2 - \beta^2$ als $a > \beta$ sein muss. Bekanntlich lässt diese Gleichung unendlich viele Auflösungen zu, allein man überzeugt sich leicht, dass nur die in den kleinsten Zahlen ausgedrückte die Bedingung $a > \beta$ erfüllt, während für alle übrigen $\beta > a$ ist. Es giebt also immer einen und nur einen sich selbst conjugirten Divisor, dem die Form $4n+1$ oder $4n+3$ zukommen wird, je nachdem die durch ihn darstellbare Zahl a von der einen oder der andern dieser Formen ist.

§. 6.

Unter den quadratischen Divisoren $4n+1$ der Form $t^2 + au^2$ befindet sich immer $t^2 + au^2$ selbst. Nach der im vorhergehenden Paragraphen festgestellten Art die quadratischen Divisoren darzustellen, müssten wir eigentlich dafür die modificirte Form:

$$t^2 + 2tu + (a+1)u^2$$

einführen; doch behalten wir der Einfachheit wegen in diesem besondern Falle $t^2 + au^2$ bei. Was nun diesen quadratischen Divisor betrifft, so lässt sich leicht zeigen, dass derselbe immer zur ersten Klasse gehört.

*) *Théorie des Nombres*, no. 217, 218.

Um dies zu beweisen, betrachten wir die Gleichung:

$$(7) \quad t^2 + au^2 = p.$$

in der p eine Primzahl $4n+1$ bezeichnet. Nimmt man zuerst t ungerade und folglich u gerade an, und setzt:

$$t = gg'g'' \dots \quad u = 2^s hkh'' \dots,$$

so kommt:

$$\left(\frac{a}{g}\right) = \left(\frac{p}{g}\right) \quad \text{oder} \quad \left(\frac{g}{a}\right) = \left(\frac{g}{p}\right),$$

woraus durch Multiplication in die ähnlichen Gleichungen für g', g'', \dots die Relation:

$$(8) \quad \left(\frac{t}{a}\right) = \left(\frac{t}{p}\right)$$

hervorgeht. Ebenso erhält man:

$$\left(\frac{p}{h}\right) = 1. \quad \text{oder} \quad \left(\frac{h}{p}\right) = 1,$$

und hieraus folgt:

$$(8^*) \quad \left(\frac{hkh'' \dots}{p}\right) = 1.$$

Ist p von der Form $8n+1$, so hat man bekanntlich $\left(\frac{2}{p}\right) = 1$ und also auch $\left(\frac{2^s}{p}\right) = 1$. Hat aber p die Form $8n+5$, so folgt aus der Gleichung (7), dass u nur durch die erste Potenz von 2 theilbar ist, d. h. dass $\beta = 1$ ist. Auf der andern Seite hat man bekanntlich in diesem Falle $\left(\frac{2}{p}\right) = -1$, oder was dasselbe ist, $\left(\frac{2^s}{p}\right) = -1$. Beide Fälle sind in der Formel:

$$\left(\frac{2^s}{p}\right) = (-1)^{\frac{p-1}{4}}$$

enthalten, die mit der Gleichung (8*) multiplicirt das Resultat giebt:

$$(9) \quad \left(\frac{u}{p}\right) = (-1)^{\frac{p-1}{4}}.$$

Eine ähnliche Untersuchung des Falls, wo t gerade und u ungerade ist, ergibt statt der Gleichungen (8) und (9) die beiden folgenden:

$$\left(\frac{t}{a}\right) = \left(\frac{t}{p}\right)(-1)^{\frac{p-1}{4}} \quad \text{und} \quad \left(\frac{u}{p}\right) = 1.$$

Verbindet man diese Gleichungen und ebenso die beiden Gleichungen (8) und (9) mit einander, so erhält man in beiden Fällen gemeinschaftliches Resultat:

$$(10) \quad \left(\frac{t}{a}\right) = \left(\frac{t}{p}\right)\left(\frac{u}{p}\right)(-1)^{\frac{p-1}{4}}.$$

Aus (7) folgt leicht:

$$t^{\frac{p-1}{2}} \equiv (-a)^{\frac{p-1}{4}} u^{\frac{p-1}{2}} \pmod{p},$$

oder:

$$\left(\frac{t}{p}\right) = \varepsilon \left(\frac{u}{p}\right)(-1)^{\frac{p-1}{4}},$$

wo wieder ε dieselbe Bedeutung wie oben hat. Ebenso erhält man:

$$t^{\frac{a-1}{2}} \equiv p^{\frac{a-1}{4}} \pmod{a}$$

oder:

$$\left(\frac{t}{a}\right) = \delta.$$

Multiplicirt man diese Ausdrücke für $\left(\frac{t}{a}\right)$ und $\left(\frac{t}{p}\right)$ in einander und vergleicht mit (10), so ergibt sich:

$$\delta = \varepsilon,$$

welche Gleichung die aufgestellte Behauptung, dass die Form $t^2 + au^2$ zur ersten Klasse gehört, rechtfertigt.

§. 7.

Wir wenden uns jetzt zur Betrachtung der conjugirten Divisoren, um zu untersuchen, wann solche zu derselben und wann sie zu entgegengesetzten Klassen gehören. Es seien zu diesem Ende p und q zwei Primzahlen $4n+1$, die respective durch zwei einander conjugirte Divisoren dargestellt werden können.

Nach der oben bemerkten Eigenschaft solcher Divisoren werden p und $2q$ demselben Divisor angehören, und mithin wird ihr Product $2pq$ in der Form $t^2 + au^2$ enthalten sein. Wir haben daher folgende Gleichung:

$$(11) \quad t^2 + au^2 = 2pq,$$

in der t und u ungerade sind.

Zerlegt man t und u in Primzahlen und setzt:

$$t = gg'g'' \dots, \quad u = hh'h'' \dots,$$

so hat man leicht aus (11):

$$\left(\frac{a}{g}\right) = \left(\frac{2pq}{g}\right) = \left(\frac{2}{g}\right)\left(\frac{p}{g}\right)\left(\frac{q}{g}\right).$$

Die Anwendung des Reciprocitätsgesetzes und eines andern bekannten Satzes giebt:

$$\left(\frac{g}{a}\right) = \pm \left(\frac{g}{p}\right)\left(\frac{g}{q}\right),$$

wo das obere oder untere Zeichen zu nehmen ist, je nachdem g die Form $8n \pm 1$ oder die Form $8n \pm 5$ hat. Multiplicirt man diese Gleichung mit den analogen für g', g'', \dots so kommt:

$$\left(\frac{t}{a}\right) = \pm \left(\frac{t}{p}\right)\left(\frac{t}{q}\right),$$

wo das obere oder das untere Zeichen gilt, je nachdem sich unter den einfachen Factoren von t eine gerade oder ungerade Anzahl von solchen befindet, die von der Form $8n \pm 5$ sind, oder was dasselbe ist, je nachdem t die Form $8n \pm 1$ oder die Form $8n \pm 5$ hat. Bemerkt man, dass $8n \pm 1$ und $8n \pm 5$ quadriert respective die Form $16n + 1$ und $16n + 9$ annehmen, so lässt sich das doppelte Zeichen durch $(-1)^{\frac{t-1}{8}}$ ausdrücken, und man hat also:

$$\left(\frac{t}{a}\right) = \left(\frac{t}{p}\right)\left(\frac{t}{q}\right)(-1)^{\frac{t-1}{8}}.$$

Auf ganz ähnliche Weise erhält man aus (11):

$$\left(\frac{u}{p}\right)\left(\frac{u}{q}\right) = (-1)^{\frac{u^2-1}{8}}.$$

Verbindet man diese Gleichungen durch Multiplication, so kommt:

$$(12) \quad \left(\frac{t}{a}\right)\left(\frac{u}{p}\right)\left(\frac{u}{q}\right) = \left(\frac{t}{p}\right)\left(\frac{t}{q}\right)(-1)^{\frac{t^2+u^2-2}{8}}.$$

Auf der andern Seite folgt aus (11):

$$t^2 \equiv -au^2 \pmod{pq},$$

und hieraus:

$$t^{\frac{p-1}{2}} \equiv (-a)^{\frac{p-1}{4}} u^{\frac{p-1}{2}} \pmod{p}, \quad t^{\frac{q-1}{2}} \equiv (-a)^{\frac{q-1}{4}} u^{\frac{q-1}{2}} \pmod{q}.$$

Führt man wieder ε und ε' , wie oben, zur Abkürzung ein, so dass:

$$a^{\frac{p-1}{4}} \equiv \varepsilon \pmod{p}, \quad a^{\frac{q-1}{4}} \equiv \varepsilon' \pmod{q},$$

so lassen sich diese Congruenzen wie folgt als Gleichungen schreiben:

$$(13) \quad \left(\frac{t}{p}\right) = \varepsilon \left(\frac{u}{p}\right) (-1)^{\frac{p-1}{4}}, \quad \left(\frac{t}{q}\right) = \varepsilon' \left(\frac{u}{q}\right) (-1)^{\frac{q-1}{4}}.$$

Auch schliesst man leicht aus (11):

$$t^2 \equiv 2pq, \quad t^{\frac{a-1}{2}} \equiv 2^{\frac{a-1}{4}} p^{\frac{a-1}{4}} q^{\frac{a-1}{4}} \pmod{a}.$$

Setzt man wie früher:

$$p^{\frac{a-1}{4}} \equiv \delta, \quad q^{\frac{a-1}{4}} \equiv \delta' \pmod{a},$$

und in ähnlichem Sinne:

$$2^{\frac{a-1}{4}} \equiv \varrho \pmod{a},$$

so wird die vorige Congruenz:

$$\left(\frac{t}{a}\right) = \delta\delta'\varrho.$$

Substituiert man diesen Ausdruck für $\left(\frac{t}{a}\right)$ und die Ausdrücke (13) für $\left(\frac{t}{p}\right)$ und $\left(\frac{t}{q}\right)$ in (12), so kommt:

$$\delta\delta'\varrho = \varepsilon\varepsilon'(-1)^{\frac{p-1}{4} + \frac{q-1}{4} + \frac{r^2+u^2-2}{8}}.$$

Zur Vereinfachung dieser Gleichung bemerke man, dass man zum Exponenten die offenbar gerade Zahl:

$$\frac{p-1}{2} \frac{q-1}{2} \quad \text{oder} \quad \frac{pq-1}{4} - \frac{p-1}{4} - \frac{q-1}{4}$$

addiren darf. Man hat also auch:

$$\delta\delta'\varrho = \varepsilon\varepsilon'(-1)^{\frac{pq-1}{4} + \frac{r^2+u^2-2}{8}}$$

oder, wenn man nach (11):

$$t^2 = 2pq - au^2$$

substituiert:

$$\delta\delta'\varrho = \varepsilon\varepsilon'(-1)^{\frac{pq-1}{2} - \frac{a-1}{8} u^2}.$$

oder endlich, da $\frac{pq-1}{2}$ gerade und a^2 ungerade ist:

$$\delta\delta'q = \varepsilon\varepsilon'(-1)^{\frac{a-1}{8}}.$$

Diese Gleichung, aus welcher folgt, dass entweder gleichzeitig:

$$\delta\delta' = \varepsilon\varepsilon' \quad \text{und} \quad q(-1)^{\frac{a-1}{8}} = 1,$$

oder gleichzeitig:

$$\delta\delta' = -\varepsilon\varepsilon' \quad \text{und} \quad q(-1)^{\frac{a-1}{8}} = -1$$

ist, zeigt, dass die beiden conjugirten Formen zu derselben oder zu verschiedenen Klassen gehören, je nachdem:

$$q(-1)^{\frac{a-1}{8}} = 1 \quad \text{oder} \quad q(-1)^{\frac{a-1}{8}} = -1$$

ist. Remmert man sich, dass $q = +1$ oder $q = -1$, je nachdem 2 biquadratischer Rest oder Nichtrest von a ist, so hängt die Entscheidung hauptsächlich davon ab, ob 2 biquadratischer Rest oder Nichtrest von a ist. Nun gilt aber für jede Primzahl a der Form $8n+1$ folgender Satz:

„Setzt man $a = g^2 + \psi^2$ (wo ψ als gerade angenommen ist), so ist 2 biquadratischer Rest oder Nichtrest von a , je nachdem ψ in der Form $8n$ oder in der Form $8n+4$ enthalten ist.“*)

Vermöge dieses Satzes hat man also $q = (-1)^{\frac{1}{2}\psi}$ oder auch, da g ungerade ist, $q = (-1)^{\frac{1}{4}\psi}$. Setzt man diesen Ausdruck und $a = g^2 + \psi^2$ in das zuletzt erhaltene Resultat, so findet man, dass conjugirte Formen zu derselben oder zu entgegengesetzten Klassen gehören, je nachdem:

$$(-1)^{\frac{(g+\psi)^2-1}{8}} = +1, \quad \text{oder} \quad (-1)^{\frac{(g+\psi)^2-1}{8}} = -1,$$

oder was dasselbe ist, je nachdem $\frac{(g+\psi)^2-1}{8}$ gerade oder ungerade ist. Bemerkte man jetzt, dass $g+\psi$ als ungerade Zahl in einer der Formen $8n \pm 1$ und $8n \pm 5$ enthalten ist, die quadriert respective in $16n+1$ und $16n+9$ übergehen, und substituirt diese successive in den Ausdruck $\frac{(g+\psi)^2-1}{8}$, so gelangt man zu folgendem Satz:

*) *Theoria residuorum biquadraticorum auct. C. F. GAUSS. Comment. primæ art. 23. I.* oder *CRELLE Journal Bd. III pag. 41*).

) S. 70 dieser Ausgabe von G. Lejeune Dirichlet's Werken.

„Setzt man $a = g^2 + \psi^2$, so gehören irgend zwei conjugirte Divisoren $4n+1$ der Form $t^2 + au^2$ zu derselben Klasse oder zu entgegengesetzten Klassen, je nachdem $g + \psi$ in der Form $8n \pm 1$ oder in der Form $8n \pm 5$ enthalten ist.“

§. 8.

Schliesslich wollen wir noch ein Kriterium dafür aufsuchen, ob der sich selbst conjugirte Divisor:

$$at^2 + 2\beta tu + 2au^2$$

der Form $4n+1$ oder der Form $4n+3$ angehört. In dem Falle, wo conjugirte Formen zu verschiedenen Klassen gehören, bietet die Frage nicht die geringste Schwierigkeit dar. Es ist klar, dass alsdann der sich selbst conjugirte Divisor die Form $4n+3$ haben muss, indem derselbe, wenn er in der Form $4n+1$ enthalten sein sollte, widersprechende Eigenschaften in sich vereinigen müsste. Wenn aber conjugirte Divisoren in derselben Klasse vereinigt sind, so erfordert die Sache eine besondere Untersuchung. Um für dieselbe einen Ausgangspunkt zu gewinnen, bemerken wir, dass in jedem Falle nach dem am Ende des §. 5 Gesagten Alles darauf ankommt, ob a in der Gleichung:

$$(14) \quad 2a^2 - \beta^2 = a$$

die Form $4n+1$ oder $4n+3$ hat.

Setzt man:

$$\alpha = gg'g'' \dots, \quad \beta = hh'h'' \dots$$

wo $g, g', \dots, h, h', \dots$ ungerade Primzahlen sind, so hat man zunächst:

$$\left(\frac{\alpha}{g}\right) = \left(\frac{-1}{g}\right)$$

und hieraus nach bekannten Sätzen:

$$\left(\frac{g}{\alpha}\right) = \pm 1,$$

wo das obere oder das untere Zeichen gilt, je nachdem g die Form $4n+1$ oder $4n+3$ hat. Multiplicirt man alle ähnlichen Gleichungen in einander, so kommt:

$$\left(\frac{\alpha}{\alpha}\right) = \pm 1.$$

wo das obere oder das untere Zeichen gilt, je nachdem unter den Primfactoren g, g', \dots von a sich eine gerade oder ungerade Anzahl in der Form $4n+3$ enthaltener befindet, oder je nachdem a selbst die Form $4n+1$ oder $4n+3$ hat. Nach dem vorher Bemerkten läuft also unsere Frage auf die Bestimmung von $\left(\frac{a}{a}\right)$ hinaus.

Kehren wir zur Gleichung (14) zurück, so ergibt dieselbe auch:

$$\left(\frac{a}{h}\right) = \left(\frac{2}{h}\right) \quad \text{oder} \quad \left(\frac{h}{a}\right) = \pm 1,$$

wo das obere oder untere Zeichen gilt, je nachdem h in der Form $8n \pm 1$ oder $8n \pm 5$ enthalten ist. Durch Multiplication erhält man wie in früheren ähnlichen Fällen:

$$\left(\frac{\beta}{a}\right) = (-1)^{\frac{\beta^2-1}{8}}.$$

Auch folgt leicht aus (14):

$$2^{\frac{a-1}{4}} \alpha^{\frac{a-1}{2}} \equiv \beta^{\frac{a-1}{2}} \pmod{a},$$

oder wenn man auf beiden Seiten mit $2^{\frac{a-1}{4}}$ multiplicirt, wie früher $\varrho \equiv 2^{\frac{a-1}{4}}$ (mod. a) setzt und sich erinnert, dass $\left(\frac{2}{a}\right) = 1$ ist:

$$\left(\frac{\alpha}{a}\right) = \varrho \left(\frac{\beta}{a}\right),$$

oder für $\left(\frac{\beta}{a}\right)$ seinen Werth gesetzt:

$$\left(\frac{\alpha}{a}\right) = \varrho (-1)^{\frac{\beta^2-1}{8}}.$$

Die Substitution von $\beta^2 = 2\alpha^2 - a$ aus (14) giebt:

$$\left(\frac{\alpha}{a}\right) = \varrho (-1)^{\frac{\alpha^2-1}{4} - \frac{a-1}{8}},$$

oder was dasselbe ist, da $\frac{\alpha^2-1}{4}$ gerade ist:

$$\left(\frac{\alpha}{a}\right) = \varrho (-1)^{\frac{a-1}{8}}.$$

Dieser Werth für $\left(\frac{a}{a}\right)$ fällt ganz mit dem Ausdruck zusammen, von dem im §. 7 die Entscheidung abhängt, ob conjugirte Divisoren derselben oder verschiedenen Klassen angehören. Wir können also das dort aus der weiteren Betrachtung dieses Ausdrucks abgeleitete Kriterium auf unsere jetzige Frage anwenden und erhalten alsdann folgenden neuen Satz:

„Setzt man $a = g^2 + \psi^2$ (wo a eine Primzahl $8n+1$), so gehört der sich selbst conjugirte quadratische Divisor von $t^2 + av^2$ der Form $4n+1$ oder $4n+3$ an, je nachdem $g + \psi$ in der Form $8n \pm 1$ oder in der Form $8n \pm 5$ enthalten ist.“

EINIGE NEUE SÄTZE
ÜBER UNBESTIMMTE GLEICHUNGEN.

VON

G. LEJEUNE DIRICHLET.

Abhandlungen der Königlich Preussischen Akademie der Wissenschaften von 1831, S. 649—664.

EINIGE NEUE SÄTZE ÜBER UNBESTIMMTE GLEICHUNGEN.

[Gelesen in der Akademie der Wissenschaften am 19. Juni 1834.]

Obgleich die Methoden zur Auflösung der unbestimmten Gleichungen des zweiten Grades mit zwei Unbekannten, welche man LAGRANGE verdankt, nichts zu wünschen übrig lassen, wenn eine solche Gleichung mit numerisch gegebenen Coefficienten wirklich aufgelöst werden soll, mag man nun für die Unbekannten bloss Rationalzahlen verlangen oder die beschränkendere Beiligung hinzufügen, dass dieselben ganze Zahlen werden sollen, so findet doch zwischen diesen beiden Fällen ein wesentlicher Unterschied statt, wenn man, ohne die Auflösung wirklich darzustellen, bloss entscheiden will, ob die vorgelegte Gleichung eine solche zulässt oder nicht. Im ersten Falle, wo die Unbekannten nur rationale Werthe zu erhalten brauchen, sind die Transformationen, welche die wirkliche Auflösung der Gleichung erfordert, von so einfacher Art, dass man aus der genauen Betrachtung derselben einen Satz hat ableiten können, welcher die Möglichkeit der Gleichung unmittelbar aus den Coefficienten zu beurtheilen erlaubt. Werden hingegen ganze Zahlen für die Unbekannten verlangt, so ist zur Entscheidung über die Möglichkeit der Gleichung, wenn ihre Coefficienten nicht etwa von solcher Beschaffenheit sind, dass sie nicht einmal einer Auflösung in blossen Rationalzahlen fähig ist, die Ausführung aller Rechnungen nöthig, welche zur wirklichen Auflösung erfordert werden.

Man wird dies wenig befremdend finden, wenn man bedenkt, dass in diesem Falle unter den vorgeschriebenen Operationen die Verwandlung der Wurzel einer quadratischen Gleichung in einen Kettenbruch vorkommt, und dass man über den Zusammenhang der Glieder eines solchen Bruchs mit den Coefficienten der Gleichung, aus der er hervorgegangen, noch ziemlich im Dunkeln ist. Doch hat man für einige Gleichungen von specieller Form Kriterien, um über ihre Möglichkeit zu entscheiden, ohne die ganze Reihe der durch die allgemeine Auflösungsmethode vorgeschriebenen Transformationen zu durch-

laufen. Zu den wenigen bekannten Sätzen, die diese Erleichterung gewähren, habe ich Gelegenheit gehabt, einige hinzuzufügen, welche ich der Akademie in dieser Abhandlung vorzulegen die Ehre habe.

Die eben erwähnten Sätze stehen im innigsten Zusammenhang mit der Gleichung:

$$t^2 - Au^2 = 1.$$

welche in der Theorie der unbestimmten Gleichungen des zweiten Grades eine so wichtige Rolle spielt. Von FERMAT nach der damaligen Mode den englischen Mathematikern vorgelegt, beschäftigte dieselbe namentlich PELL und Lord BROUNKER, deren Auflösungen in die Lehrbücher der Algebra von WALLIS und EULER übergingen. Ihre eigentliche Wichtigkeit erhielt jedoch diese Gleichung erst durch die von EULER gemachte Bemerkung, dass mit Hülfe derselben aus einer bekannten Auflösung einer Gleichung des zweiten Grades neue Auflösungen in unendlicher Anzahl abgeleitet werden können. Diese Eigenschaft (die aller Wahrscheinlichkeit nach schon FERMAT bekannt war, und durch die er vielleicht auf die Gleichung selbst geführt worden war) machte es für die weitere Ausbildung dieses Theils der Analysis nothwendig, streng nachzuweisen, was man bis dahin stillschweigend vorausgesetzt hatte, dass die obige Gleichung für jeden nicht quadratischen Werth von A eine Auflösung zulässt; denn, wiewohl die BROUNKER'sche und PELL'sche Methode in jedem besondern Falle zur Auflösung führte, und, wie wir jetzt wissen, nothwendig führen musste (da sie von der jetzt gebräuchlichen Methode nicht wesentlich verschieden ist), so ging doch diese Nothwendigkeit nicht unmittelbar aus der Natur der Methode selbst hervor, und es konnte mit Recht gezeifelt werden, ob die Gleichung unter der oben ausgesprochenen Beschränkung immer möglich sei. LAGRANGE hob jeden Zweifel, indem er die Theorie der Kettenbrüche auf diese Frage anwandte, und legte so den Grund zu der vollständigen Behandlung der unbestimmten Gleichungen des zweiten Grades.

Was nun die früher erwähnten Kriterien betrifft, welche LEGENDRE aus der für jedes A stattfindenden Lösbarkeit der FERMAT'schen Gleichung abgeleitet hat, so geben dieselben unter andern auch über die für einige Untersuchungen wichtige Frage, für welche Werthe von A die Gleichung:

$$t^2 - Au^2 = -1$$

eine Auflösung zulässt, in mehreren Fällen Aufschluss. LAGRANGE hatte in

seiner ersten Abhandlung über unbestimmte Gleichungen*), von einer nicht weit genug fortgesetzten Induction verleitet, die Vermuthung ausgesprochen, dass die vorhergehende Gleichung stets möglich sei, wenn A keine anderen ungeraden Primfactoren enthält als solche von der Form $4n+1$. Diese Bedingung ist nöthig, indem sonst A kein Divisor von l^2+1 sein könnte, wie es die Gleichung erfordert, allein sie reicht nicht hin und ist z. B. für $A = 5.41$ erfüllt, ohne dass deshalb die Gleichung eine Auflösung zulässt. Man kann zwar mehrere Bedingungen auffinden, welche die Auflösbarkeit der Gleichung zur Folge haben, aber sie erschöpfen nicht alle Fälle, und es scheint eine sehr schwierige Aufgabe zu sein, das vollständige Merkmal anzugeben, woran sich alle Werthe von A erkennen lassen, für welche die Gleichung möglich ist.

§. 1.

Wir beginnen mit einer kurzen Darstellung der LEGENDRE'schen Methode**). Es bezeichne A eine gegebene positive Zahl ohne quadratischen Factor, d. h. deren Primfactoren alle von einander verschieden sind, und es seien p und q die kleinsten Werthe ($p = 1$ und $q = 0$ ausgenommen), welche der bekanntlich immer lösbaren Gleichung:

$$(1) \quad p^2 - Aq^2 = 1$$

genügen. Bringt man dieselbe in die Form $(p+1)(p-1) = Aq^2$, und bemerkt man, dass $p+1$ und $p-1$ relative Primzahlen sind oder bloss den gemeinschaftlichen Factor 2 haben, je nachdem p gerade oder ungerade ist, so sieht man gleich, dass die Gleichung (1) im ersten Falle die folgenden nach sich zieht:

$$p+1 = Mr^2, \quad p-1 = Ns^2, \quad A = MN, \quad q = rs,$$

und ebenso im zweiten:

$$p+1 = 2Mr^2, \quad p-1 = 2Ns^2, \quad A = MN, \quad q = 2rs,$$

wo M , N und mithin r , s durch p völlig bestimmt sind. Es sind nämlich M , N im ersten Falle respective die grössten gemeinschaftlichen Theiler von A , $p+1$ und A , $p-1$, im andern dagegen von A , $\frac{p+1}{2}$ und A , $\frac{p-1}{2}$. Aus diesen Gleichungen folgt resp. für den ersten und zweiten Fall:

$$(2) \quad Mr^2 - Ns^2 = 2, \quad Mr^2 - Ns^2 = 1.$$

*) *Mélanges de Turin. Tome IV, seconde partie, p. 88.*

***) *Théorie des Nombres, première partie, §. VII.*

Hat man die Gleichung (1) nicht wirklich aufgelöst, und ist also p nicht bekannt, so weiss man bloss, dass eine dieser Gleichungen stattfinden muss, und da unter dieser Voraussetzung M und N nicht einzeln gegeben sind, so enthält jede der Gleichungen (2) mehrere besondere Gleichungen, die man erhält, indem man successive für M alle Factoren von A (1 und A mit eingeschlossen) nimmt und $N = \frac{A}{M}$ setzt. Das LEGENDRE'sche Verfahren besteht nun darin, eine oder mehrere dieser Gleichungen als unmöglich nachzuweisen. Bleibt nach dieser Ausschliessung nur eine übrig, so ist die Lösbarkeit derselben dargethan; im anderen Falle ist nicht entschieden, welche unter den nicht ausgeschlossenen stattfindet*). Es lässt sich immer allgemein, d. h. für jedes A , eine Gleichung angeben, welche ausgeschlossen werden muss, diejenige nämlich, welche die zweite Gleichung (2) für den Fall darstellt, wo man $M = 1$ setzt; denn, da diese der Form nach mit (1) zusammenfällt, und da r und s offenbar resp. kleiner als p und q sind, so würde aus derselben gegen die gemachte Voraussetzung folgen, dass man nicht von der in den kleinsten Zahlen ausgedrückten Auflösung der Gleichung (1) ausgegangen ist.

§. 2.

Es sei nun, um das eben angedeutete Verfahren anzuwenden, A zunächst eine ungerade Primzahl. Die Gleichungen (2) reduciren sich alsdann auf die folgenden:

$$r^2 - As^2 = 2, \quad Ar^2 - s^2 = 2, \quad Ar^2 - s^2 = 1.$$

Hat A die Form $4n+1$, so sind die beiden ersten unmöglich, da in

*) Es geht aus dem Gesagten bloss hervor, dass von sämmtlichen Gleichungen (2) (welche man durch alle möglichen Zerfällungen von A in zwei Factoren M und N erhält) immer nur eine aus (1) folgt. Man könnte daher vermuthen, dass von allen diesen Gleichungen, wenn man von ihrem Ursprung aus (1) abstirbt, d. h. r und s in denselben als ganz unbestimmte Zahlen betrachtet, mehrere möglich werden können. In diesem Falle müssten diese möglichen Gleichungen nach Anwendung irgend einer Ausschliessungsmethode übrig bleiben, insofern nämlich dabei die Gleichungen ebenfalls an und für sich betrachtet würden. Allein es ist leicht, jede Ungewissheit zu heben, denn man kann beweisen (man sehe das Ende der Abhandlung), dass von den Gleichungen (2), wenn man auch r und s in denselben ganz unbestimmt lässt, ausser der immer darunter befindlichen $r^2 - As^2 = 1$, die nun nicht mehr auszuschliessen ist, nur noch eine einzige möglich ist. Wenn daher das LEGENDRE'sche Verfahren und die im Folgenden entwickelte Methode ausser dieser noch mehr als eine Gleichung übrig lassen, so liegt die dadurch entstehende Unbestimmtheit nicht in der Natur der Sache, und es sind neue Kriterien erforderlich, um unter diesen Gleichungen diejenige zu erkennen, welche allein eine Auflösung zulässt.

beiden die erste Seite offenbar nicht gerade sein kann, ohne durch 4 theilbar zu werden. Die dritte bleibt also allein übrig, und man erhält den Satz:

„Für jede Primzahl A der Form $4n+1$ ist die Gleichung $t^2 - An^2 = -1$ möglich.“

Ist A von der Form $4n+3$, welche in die beiden Unterabtheilungen $8n+3$, $8n+7$ zerfällt, so ist die dritte nicht zulässig, da nach derselben A ein Theiler von s^2+1 sein müsste, welche Eigenschaft keiner Primzahl dieser Form zukommt. Zugleich ist klar, dass, da in den beiden ersten r und s ungerade vorausgesetzt werden müssen und jedes ungerade Quadrat in der Form $8n+1$ enthalten ist, die ersten Seiten derselben resp. die Formen $8n+6$, $8n+2$ oder die Formen $8n+2$, $8n+6$ annehmen werden, je nachdem A in der Form $8n+3$ oder in der Form $8n+7$ enthalten ist. Vergleicht man diese Formen mit dem Werthe der zweiten Seite, so ergibt sich der Satz:

„Für jede Primzahl A der Form $8n+7$ ist die Gleichung $t^2 - An^2 = 2$, für jede Primzahl A der Form $8n+3$ hingegen die Gleichung $t^2 - An^2 = -2$ möglich.“

Man sieht also, dass man nie ungewiss ist, welche Gleichung stattfindet, wenn A eine Primzahl ist. Anders stellt sich die Sache, wenn A mehrere einfache Factoren enthält. Setzt man $A = 2a$, wo a irgend eine ungerade Primzahl bezeichnet, so ist p ungerade, und man erhält aus der zweiten Gleichung (2) die folgenden:

$$2r^2 - as^2 = 1, \quad ar^2 - 2s^2 = 1, \quad 2ar^2 - s^2 = 1.$$

Hat a die Form $4n+3$, so ist wieder die letzte auszuschliessen, weil a kein Theiler von s^2+1 sein kann. Ist $a = 8n+3$, so ist auch die erste nicht möglich, da die erste Seite, wenn sie ungerade sein soll, nur eine der Formen $8n+5$, $8n+7$ annehmen kann. Ganz ähnlicher Weise ist für $a = 8n+7$ die zweite auszuschliessen. Es folgt also der Satz:

„Die Gleichung $2t^2 - an^2 = 1$ gilt für jede Primzahl a der Form $8n+7$, die Gleichung $2t^2 - an^2 = -1$ hingegen für jede Primzahl a der Form $8n+3$.“

Untersucht man jetzt den Fall, wo $a = 4n+1$, so kann die dritte nicht mehr ausgeschlossen werden. Hat a die speciellere Form $8n+5$, so sind die beiden ersten nicht möglich, denn in jeder derselben kann die erste Seite, wenn sie ungerade bleiben soll, nur eine der Formen $8n+3$, $8n+5$ annehmen. Wir haben also den Satz:

„Ist a eine Primzahl der Form $8n+5$, so findet die Gleichung $t^2 - 2au^2 = -1$ immer statt.“

Für den Fall hingegen, wo man a die Form $8n+1$ beilegt, ergibt diese Ausschliessungsmethode gar kein Resultat, und es bleibt völlig unentschieden, welche der drei Gleichungen stattfinden muss. Auf diesen Fall wollen wir nun die Methode anwenden, welche den eigentlichen Gegenstand dieser Abhandlung ausmacht. Wir werden zeigen, dass, sobald a gewisse Bedingungen erfüllt, die beiden ersten der zu untersuchenden Gleichungen, welche wir zu leichterer Uebersicht in der Doppelgleichung:

$$2t^2 - au^2 = \pm 1$$

vereinigen, nicht stattfinden können. Wir nehmen zunächst das obere Zeichen und haben also die Gleichung:

$$(3) \quad 2t^2 - au^2 = 1$$

zu untersuchen. Zerlegt man u , welches offenbar ungerade ist, in seine einfachen Factoren h, h', h'', \dots , so dass $u = hh'h'' \dots$, so ergibt diese Gleichung auf der Stelle, wenn man sich des von LEGENDRE eingeführten Zeichens bedient:

$$\left(\frac{2}{h}\right) = 1, \quad \left(\frac{2}{h'}\right) = 1, \quad \left(\frac{2}{h''}\right) = 1, \quad \dots$$

Jede der Primzahlen h, h', h'' , ist also nach bekannten Sätzen in einer der Formen $8n+1, 8n-1$ enthalten, und dasselbe gilt also auch von ihrem Product u .

Aus der für u gefundenen Form $8n \pm 1$ folgt für u^2 die Form $16n+1$, und da t offenbar ungerade, $2t^2$ mithin in der Form $16n+2$ enthalten ist, so ergibt sich gleich, dass die erste Seite von (3) entweder die Form $16n+1$ oder $16n+9$ hat, je nachdem $a = 16n+1$ oder $= 16n+9$. Im letzten Falle ist daher die Gleichung (3) nicht möglich.

Nehmen wir jetzt das untere Zeichen, so haben wir folgende Gleichung zu betrachten:

$$(4) \quad 2t^2 - au^2 = -1,$$

in der t gerade angenommen werden muss. Setzt man $t = 2'gg'y'' \dots$, wo g, g', g'', \dots ungerade Primzahlen bezeichnen, so folgt aus (4):

$$\left(\frac{a}{g}\right) = 1,$$

und hieraus vermöge des Reciprocitätsgesetzes, da $a = 4n + 1$:

$$\left(\frac{g}{a}\right) = 1,$$

und ebenso:

$$\left(\frac{g'}{a}\right) = 1, \quad \left(\frac{g''}{a}\right) = 1, \quad \dots$$

Zugleich ist, da a die Form $8n + 1$ hat, $\left(\frac{2^v}{a}\right) = 1$. Man erhält also durch Multiplication:

$$\left(\frac{t}{a}\right) = 1.$$

Aus (4) ergibt sich, wenn man zur Potenz $\frac{a-1}{4}$ erhebt und berücksichtigt, dass a von der Form $8n + 1$ ist, $2^{\frac{a-1}{4}} t^{\frac{a-1}{2}} \equiv 1 \pmod{a}$, oder durch Vergleichung mit dem oben gefundenen Resultate:

$$2^{\frac{a-1}{4}} \equiv 1 \pmod{a}.$$

Ist daher $2^{\frac{a-1}{4}} \equiv -1 \pmod{a}$, so kann die Gleichung (4) nicht stattfinden.

Sind die beiden Bedingungen, welche respective die Unmöglichkeit von (3) und (4) nach sich ziehen, vereinigt, so bleibt bloss die erste Gleichung übrig, und wir erhalten so den folgenden Satz:

„Ist a eine Primzahl der Form $16n + 9$, und ist zugleich $2^{\frac{a-1}{4}} \equiv -1 \pmod{a}$, so ist die Gleichung $t^2 - 2at^2 = -1$ stets auflösbar.“

Die Entscheidung des Zeichens in $2^{\frac{a-1}{4}} \equiv \pm 1 \pmod{a}$ kann nach einem bekannten Satz durch Zerlegung von a in zwei Quadrate geschehen. Setzt man $a = g^2 + \psi^2$ (wo ψ gerade angenommen wird), so findet das obere oder untere Zeichen statt, je nachdem ψ die Form $8n$ oder die Form $8n + 4$ hat.

Es sei z. B.:

$$a = 761 = 16 \cdot 47 + 9 = 19^2 + 20^2.$$

Die Gleichung $t^2 - 1522a^2 = -1$ ist also möglich.

Die beiden Bedingungen sind jedoch nicht notwendig zur Möglichkeit der Gleichung $t^2 - 2at^2 = -1$, und diese kann eine Auflösung zulassen, ohne dass auch nur eine derselben erfüllt ist. Es ist z. B. $15^2 - 2 \cdot 113 \cdot 1^2 = -1$, und doch ist 113 von der Form $16n + 1$ und zugleich $2^{\frac{113-1}{4}} \equiv 1 \pmod{113}$. Für die Primzahlen $8n + 1$, die nicht beiden Bedingungen zugleich genügen,

sind also neue Kriterien erforderlich, zu deren Entdeckung das hier gebrauchte Verfahren nicht geeignet scheint.

§. 3.

Wir behandeln jetzt den Fall, wo A das Product von zwei ungeraden Primzahlen a , b ist, die entweder beide die Form $4n+1$ oder beide die Form $4n+3$ haben: die Gleichungen werden für diesen Fall:

$$\begin{aligned} r^2 - abs^2 = 2, \quad ar^2 - bs^2 = 2, \quad br^2 - as^2 = 2, \quad abr^2 - s^2 = 2, \\ ar^2 - bs^2 = 1, \quad br^2 - as^2 = 1, \quad abr^2 - s^2 = 1. \end{aligned}$$

Die vier ersten sind nicht zulässig, da nach den gemachten Voraussetzungen in jeder derselben die erste Seite, wenn sie gerade sein soll, durch 4 theilbar wird. Sind a und b beide $4n+3$, so ist auch $abr^2 - s^2 = 1$ auszuschliessen, und es entscheidet sich gleich, welche der beiden anderen stattfindet, denn die Existenz der ersten erfordert die Bedingung $\left(\frac{a}{b}\right) = 1$, und ebenso die der zweiten $\left(\frac{-a}{b}\right) = 1$, oder was dasselbe ist, $\left(\frac{a}{b}\right) = -1$.

Es gilt also folgender Satz:

„Sind a und b zwei Primzahlen $4n+3$, so ist die Gleichung $at^2 - bn^2 = \pm 1$ immer möglich, wo das Zeichen mit dem des Ausdrucks $\left(\frac{a}{b}\right) = \pm 1$ übereinstimmt.“

Haben a und b die Form $4n+1$, so ist die letzte Gleichung nicht mehr auszuschliessen. Soll die erste stattfinden, so müssen die Bedingungen $\left(\frac{a}{b}\right) = 1$ und $\left(\frac{-b}{a}\right) = \left(\frac{b}{a}\right) = 1$ erfüllt sein. Nach dem Reciprocitätsgesetz reduciren sich dieselben auf eine von beiden, da immer für Primzahlen der genannten Form $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)$ ist. Dieselbe Bedingung $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right) = 1$ ist zur Möglichkeit der zweiten Gleichung erforderlich. Es folgt also hieraus der Satz:

„Sind a und b zwei Primzahlen $4n+1$ und hat man zugleich $\left(\frac{a}{b}\right) = -1$, so ist die Gleichung $t^2 - abn^2 = -1$ immer möglich.“

Ist hingegen $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right) = 1$, so bleibt es auf diese Weise unentschieden, welche der drei übrig bleibenden Gleichungen eine Auflösung zulässt. Um für

diesen Fall Kriterien zu finden, wenden wir das vorher gebrauchte Verfahren auf die beiden ersten dieser Gleichungen an, und ziehen dieselben zu grösserer Gleichförmigkeit der Bezeichnung in die folgende zusammen:

$$at^2 - bu^2 = \pm 1.$$

Gilt zunächst das obere Zeichen, haben wir also die Gleichung:

$$(5) \quad at^2 - bu^2 = 1$$

zu untersuchen, so müssen t und u respective ungerade und gerade angenommen werden. Man setze $u = 2^r h h' h'' \dots$, wo h, h', h'', \dots ungerade Primzahlen bezeichnen. Aus (5) folgt leicht:

$$\left(\frac{a}{h}\right) = 1,$$

und hieraus mit Hülfe des Reciprocitätsgesetzes:

$$\left(\frac{h}{a}\right) = 1.$$

Multipliziert man diese Gleichung und die ähnlichen für h', h'', \dots , so kommt:

$$\left(\frac{h h' h'' \dots}{a}\right) = 1.$$

Die Zahl a hat eine der beiden Formen $8n+1, 8n+5$. Im ersten Falle ist

$\left(\frac{2}{a}\right) = 1$ und also auch $\left(\frac{2^r}{a}\right) = 1$. Für $a = 8n+5$ hat at^2 dieselbe Form

(da $t^2 = 8n+1$), und man sieht leicht aus (5), dass u nicht durch 4 theilbar

ist. Man hat also $\left(\frac{2^r}{a}\right) = \left(\frac{2}{a}\right) = -1$. Beide Resultate sind in der Formel:

$$\left(\frac{2^r}{a}\right) = (-1)^{\frac{a-1}{4}}$$

enthalten, und man erhält durch Multiplication mit der oben gefundenen:

$$(6) \quad \left(\frac{u}{a}\right) = (-1)^{\frac{a-1}{4}}.$$

Andrerseits folgt aus (5), wenn man zur Potenz $\frac{a-1}{4}$ erhebt:

$$b^{\frac{a-1}{4}} u^{\frac{a-1}{2}} \equiv (-1)^{\frac{a-1}{4}} \pmod{a},$$

oder, wenn man hiermit das eben erhaltene Resultat (6) vergleicht:

$$b^{\frac{a-1}{4}} \equiv 1 \pmod{a}.$$

Diese Bedingung muss also erfüllt sein, wenn die Gleichung (5) möglich sein soll. Hat man daher $b^{\frac{a-1}{4}} \equiv -1 \pmod{a}$, so ist diese Gleichung anzuschliessen. Ebenso findet man (ohne alle neue Rechnung durch blossen Vertauschung von a und b), dass die Gleichung $at^2 - bt^2 = -1$ unmöglich ist, wenn $a^{\frac{b-1}{4}} \equiv -1 \pmod{b}$. Man erhält also, wenn man beide Bedingungen als gleichzeitig stattfindend voraussetzt, folgenden Satz*):

„Sind a und b zwei Primzahlen $4n+1$, für welche $\left(\frac{a}{b}\right) = 1$, und zugleich $\left(\frac{a}{b}\right)_4 = -1$, $\left(\frac{b}{a}\right)_4 = -1$, so ist die Gleichung $t^2 - abn^2 = -1$ immer auflösbar.“

Setzt man z. B. $a = 5$, $b = 89$, so sind alle Bedingungen erfüllt. Die Gleichung $t^2 - 5 \cdot 89n^2 = -1$ lässt also eine Auflösung zu, und man findet in der That für die kleinsten Werthe von t und u :

$$t = 4662, \quad u = 221.$$

Es gilt übrigens hier wieder die schon früher gemachte Bemerkung, dass die Gleichung sehr wohl möglich sein kann, wenn gleich von den Bedingungen $\left(\frac{a}{b}\right)_4 = -1$ und $\left(\frac{b}{a}\right)_4 = -1$ keine oder nur eine erfüllt ist.

Es ist z. B. für $a = 5$, $b = 521$, $\left(\frac{a}{b}\right)_4 = 1$ und $\left(\frac{b}{a}\right)_4 = 1$, und doch ist die Gleichung $t^2 - 5 \cdot 521n^2 = -1$ auflösbar, denn man findet $t = 66402$, $u = 1301$. Ein zweites Beispiel liefert die Gleichung:

$$1040^2 - 617 \cdot 1753 \cdot 1^2 = -1, \quad \left(\frac{1753}{617}\right)_4 = 1.$$

§. 4.

Wir überlassen dem Leser die Entwicklung des Falles, wo $A = ab$, und von den Zahlen a und b die eine die Form $4n+1$, die andere die Form $4n+3$ hat, so wie des Falles, wo $A = 2ab$, und a, b ungerade Primzahlen bezeichnen, und wählen als letztes Beispiel der Anwendung unserer Methode den Fall, wenn

*) Zur Abkürzung bediene ich mich hier und im Folgenden eines dem Legendre'schen ganz ähnlichen Zeichens. Es sei c irgend eine Primzahl $4n+1$ und k eine nicht durch c theilbare Zahl, für welche $\left(\frac{k}{c}\right) = 1$, d. h. $k^{\frac{c-1}{2}} \equiv 1 \pmod{c}$; so ist entweder $k^{\frac{c-1}{4}} \equiv +1$ oder $k^{\frac{c-1}{4}} \equiv -1 \pmod{c}$. Diesen Rest $+1$ oder -1 werde ich durch $\left(\frac{k}{c}\right)_4$ bezeichnen.

A das Product von drei Primzahlen a, b, c ist, die alle drei in der Form $4n+1$ enthalten sind. Von den Gleichungen (2) sind alsdann diejenigen, deren zweite Seite 2 ist, auszuschliessen, da in denselben die erste Seite, wenn sie gerade sein soll, offenbar den Factor 4 enthält, und die übrigen lassen sich wie folgt schreiben:

$$(7) \quad \begin{cases} at^2 - bcu^2 = \pm 1, & bt^2 - acu^2 = \pm 1. \\ ct^2 - abu^2 = \pm 1, & t^2 - abc u^2 = -1. \end{cases}$$

Hat von den drei Ausdrücken:

$$\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right), \quad \left(\frac{a}{c}\right) = \left(\frac{c}{a}\right), \quad \left(\frac{b}{c}\right) = \left(\frac{c}{b}\right),$$

keiner oder nur einer den Werth $+1$, so sind alle drei Doppelgleichungen unmöglich. Aus $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right) = -1$ z. B. folgt die Unmöglichkeit der ersten und zweiten, ebenso aus $\left(\frac{a}{c}\right) = \left(\frac{c}{a}\right) = -1$ die der dritten.

„Sind a, b, c Primzahlen der Form $4n+1$, und ist zugleich von den Resten $\left(\frac{a}{b}\right), \left(\frac{b}{c}\right), \left(\frac{c}{a}\right)$, keiner oder nur einer $+1$, so ist die Gleichung $t^2 - abc u^2 = -1$ immer möglich.“

Für die beiden anderen Fälle, wo die Reste $\left(\frac{a}{b}\right), \left(\frac{b}{c}\right), \left(\frac{c}{a}\right)$ sämmtlich oder zwei derselben den Werth $+1$ haben, ist also eine neue Untersuchung nöthig. Wir beginnen mit dem zweiten, d. h. wir gehen von folgenden Voraussetzungen aus:

$$\left(\frac{a}{b}\right) = 1, \quad \left(\frac{b}{c}\right) = -1, \quad \left(\frac{c}{a}\right) = 1.$$

Die zweite und dritte Doppelgleichung kann dann offenbar nicht stattfinden, und es bleibt bloss die erste zu untersuchen. Nimmt man zunächst das obere Zeichen, so dass:

$$(8) \quad at^2 - bcu^2 = 1$$

ist, so müssen t und u respective ungerade und gerade angenommen werden.

Setzt man $u = 2^r h h' h'' \dots$, wo wieder h, h', h'', \dots ungerade Primzahlen bezeichnen, so folgt aus (8):

$$\left(\frac{a}{h}\right) = 1$$

und mit Hilfe des Reciprocitätsgesetzes:

$$\left(\frac{h}{a}\right) = 1.$$

Multipliziert man diese Gleichung in die ähnlichen für h', h'', \dots , so kommt:

$$\left(\frac{hh'h''\dots}{a}\right) = 1.$$

Hat die Primzahl a die Form $8n+1$, so ist $\left(\frac{2}{a}\right) = 1$ und also auch $\left(\frac{2^v}{a}\right) = 1$; ist hingegen $a = 8n+5$, so hat man $\left(\frac{2}{a}\right) = -1$. In diesem Falle erhellt aus (8), dass u nicht durch 4 theilbar sein kann. Es ist also $v = 1$, d. h. $\left(\frac{2^v}{a}\right) = \left(\frac{2}{a}\right) = -1$. Beide Fälle vereinigt der Ausdruck:

$$\left(\frac{2^v}{a}\right) = (-1)^{\frac{a-1}{4}},$$

und man erhält, wenn man denselben in das vorbergehende Resultat multiplicirt:

$$\left(\frac{u}{a}\right) = (-1)^{\frac{a-1}{4}}.$$

Aus (8) folgt durch Erhebung zur Potenz $\frac{a-1}{4}$:

$$\left(\frac{bc}{a}\right)_4 \left(\frac{u}{a}\right) = (-1)^{\frac{a-1}{4}}$$

und folglich:

$$\left(\frac{bc}{a}\right)_4 = 1.$$

Diese Bedingung muss also nothwendig erfüllt sein, wenn die Gleichung (8) möglich sein soll, und diese Gleichung ist auszuschliessen, sobald $\left(\frac{bc}{a}\right)_4 = -1$, oder was dasselbe ist, $\left(\frac{b}{a}\right)_4 = -\left(\frac{c}{a}\right)_4$.

Lässt man jetzt das andere Zeichen gelten, so ist die zu untersuchende Gleichung:

$$(9) \quad at^2 - bu^2 = -1.$$

wobei t und u respective gerade und ungerade anzunehmen sind. Man setze:

$$t = 2^u g g' g'' \dots$$

so erhält man gleich:

$$\left(\frac{bc}{g}\right) = \left(\frac{b}{g}\right) \left(\frac{c}{g}\right) = 1$$

und nach dem Reciprocitätsgesetz:

$$\left(\frac{g}{b}\right)\left(\frac{g}{c}\right) = 1.$$

Diese Gleichung, mit den ähnlichen für g' , g'' , ... multiplicirt, führt zu dem Resultate:

$$\left(\frac{gg'g''\dots}{b}\right)\left(\frac{gg'g''\dots}{c}\right) = 1.$$

Haben die Zahlen b und c beide die Form $8n+1$ oder beide die Form $8n+5$, so ist $\left(\frac{2}{b}\right)\left(\frac{2}{c}\right) = 1$, und also auch $\left(\frac{2^u}{b}\right)\left(\frac{2^u}{c}\right) = 1$. Ist aber eine derselben von der Form $8n+1$, während die andere von der Form $8n+5$ ist, so hat man $\left(\frac{2}{b}\right)\left(\frac{2}{c}\right) = -1$. Zugleich ist aus (9) klar, dass alsdann $\mu = 1$ ist. Man hat also für diesen Fall $\left(\frac{2^u}{b}\right)\left(\frac{2^u}{c}\right) = -1$. Multiplicirt man die Formel:

$$\left(\frac{2^u}{b}\right)\left(\frac{2^u}{c}\right) = (-1)^{\frac{u-2}{4}},$$

welche beide Resultate vereinigt, in die vorher gefundene, so findet man:

$$\left(\frac{t}{b}\right)\left(\frac{t}{c}\right) = (-1)^{\frac{b+c-2}{4}}.$$

Auf der andern Seite folgt leicht aus (9), wenn man zur Potenz $\frac{b-1}{4}$ und $\frac{c-1}{4}$ erhebt:

$$\left(\frac{a}{b}\right)_4\left(\frac{t}{b}\right) = (-1)^{\frac{t-1}{4}}, \quad \left(\frac{a}{c}\right)_4\left(\frac{t}{c}\right) = (-1)^{\frac{t-1}{4}}.$$

Vergleicht man das Product dieser Ausdrücke mit dem vorher erhaltenen, so gelangt man zu der für die Möglichkeit der Gleichung (9) nothwendigen Bedingung:

$$\left(\frac{a}{b}\right)_4\left(\frac{a}{c}\right)_4 = 1.$$

Man weiss also, dass die Gleichung (9) nicht zulässig ist, sobald $\left(\frac{a}{b}\right)_4\left(\frac{a}{c}\right)_4 = -1$. Combinirt man diese Resultate, so erhält man den Satz:

„Sind a , b , c Primzahlen $4n+1$ von solcher Beschaffenheit, dass:

$$\left(\frac{b}{a}\right) = \left(\frac{c}{a}\right) = 1, \quad \left(\frac{b}{c}\right) = -1.$$

und zugleich:

$$\left(\frac{bc}{a}\right)_4 = -1 \quad \text{und} \quad \left(\frac{a}{b}\right)_4 \left(\frac{a}{c}\right)_4 = -1,$$

so ist die Gleichung $t^2 - abc n^2 = -1$ auflösbar.*

Sämmtliche Bedingungen sind erfüllt, wenn man $a = 5$, $b = 41$, $c = 109$ annimmt, denn man hat:

$$\begin{aligned} \left(\frac{41}{5}\right) &= 1, \quad \left(\frac{109}{5}\right) = 1, \quad \left(\frac{109}{41}\right) = -1, \\ \left(\frac{41}{5}\right)_4 &= 1, \quad \left(\frac{109}{5}\right)_4 = -1, \quad \left(\frac{5}{41}\right)_4 = -1, \quad \left(\frac{5}{109}\right)_4 = 1. \end{aligned}$$

Die Gleichung $t^2 - 5 \cdot 41 \cdot 109 n^2 = -1$ ist also auflösbar. Dasselbe gilt von der Gleichung $t^2 - 5 \cdot 29 \cdot 101 n^2 = -1$.

Der andere Fall, wo nämlich die Reste $\left(\frac{a}{b}\right)$, $\left(\frac{b}{c}\right)$, $\left(\frac{c}{a}\right)$ alle drei $+1$ sind, ist einer ähnlichen Behandlung fähig. Die beiden alsdann hinzutretenden Doppelgleichungen aus (7) sind von derselben Form wie die eben untersuchte, und man erhält, wenn man die vorher gefundenen Resultate durch blosse Vertauschung von a , b , c auf dieselben überträgt, einen Satz, der sich, wie folgt, aussprechen lässt:

Sind a , b , c Primzahlen $4n+1$, welche die Bedingungen:

$$\begin{aligned} \left(\frac{a}{b}\right) &= \left(\frac{b}{c}\right) = \left(\frac{c}{a}\right) = 1, \\ \left(\frac{bc}{a}\right)_4 &= \left(\frac{ac}{b}\right)_4 = \left(\frac{ab}{c}\right)_4 = \left(\frac{a}{b}\right)_4 \left(\frac{a}{c}\right)_4 = \left(\frac{b}{a}\right)_4 \left(\frac{b}{c}\right)_4 = \left(\frac{c}{a}\right)_4 \left(\frac{c}{b}\right)_4 = -1 \end{aligned}$$

erfüllen, so ist die Gleichung $t^2 - abc n^2 = -1$ immer möglich.*

So ist z. B. die Gleichung $t^2 - 5 \cdot 41 \cdot 409 n^2 = -1$ auflösbar, denn man hat:

$$\left(\frac{41}{5}\right) = \left(\frac{409}{5}\right) = \left(\frac{409}{41}\right) = 1,$$

und:

$$\begin{aligned} \left(\frac{41}{5}\right)_4 &= 1, \quad \left(\frac{409}{5}\right)_4 = -1, \quad \left(\frac{409}{41}\right)_4 = 1, \\ \left(\frac{5}{41}\right)_4 &= -1, \quad \left(\frac{5}{409}\right)_4 = 1, \quad \left(\frac{41}{409}\right)_4 = -1. \end{aligned}$$

§. 5.

Es bleibt uns die oben in der Note zu §. 1 ausgesprochene Behauptung zu rechtfertigen. Zu diesem Zwecke bemerke man, dass die Anwendung des in dem genannten Paragraphen gebrauchten Verfahrens nicht auf die in den

kleinsten Zahlen ausgedrückte Auflösung der Gleichung (1) beschränkt ist, sondern dass man ebenso gut von irgend einer anderen Auflösung ausgehen kann. Es seien P, Q irgend zwei Werthe, die der Gleichung genügen, so dass also:

$$(10) \quad P^2 - A Q^2 = 1,$$

während man p, q wie früher zur Bezeichnung der kleinsten Werthe beibehält, so folgt ganz auf dieselbe Weise aus (10) eine der Gleichungen:

$$(11) \quad M'R^2 - N'S^2 = 2,$$

$$(12) \quad M'R^2 - N'S^2 = 1,$$

wo M', N' mit Accenten versehen sind, um sie von M, N in (2) zu unterscheiden. Es ist immer $M'N' = A$, und die erste oder zweite Gleichung gilt, je nachdem P gerade oder ungerade ist. Die Zahlen M', N' sind im ersten Falle die grössten gemeinschaftlichen Theiler von $P+1, A$ und $P-1, A$, im andern von $\frac{P+1}{2}, A$ und $\frac{P-1}{2}, A$. Umgekehrt führt jede Auflösung einer der Gleichungen (11) und (12) zu einer Auflösung von (10); denn findet (11) statt, so darf man nur $P = M'R^2 - 1$ und $Q = RS$ setzen. Findet hingegen (12) statt, so setze man $P = 2M'R^2 - 1$, und $Q = 2RS$.

Es geht hieraus hervor, dass man alle Auflösungen sowohl der Gleichungen von der Form (11) als derjenigen von der Form (12) erhalten wird, wenn man nach einander alle Werthe P, Q betrachtet, die (10) genügen. Will man, ohne alle diese Auflösungen darzustellen, bloss entscheiden, welche der in (11) und (12) enthaltenen Gleichungen auflösbar sind, so hat man nur zu untersuchen, ob P gerade oder ungerade ist, und M' zu bestimmen. Je nachdem P gerade oder ungerade ist, gehört die entsprechende Gleichung zu (11) oder (12), und der grösste gemeinschaftliche Divisor von A und $P+1$ im ersten Falle und der von A und $\frac{P+1}{2}$ im zweiten giebt den Werth von M' . Um nun sämtliche Auflösungen von (10) auf einmal zu umfassen, erinnere man sich, dass alle Werthe von P durch die Gleichung:

$$P = \frac{(p+q\sqrt{A})^n + (p-q\sqrt{A})^n}{2}$$

gegeben werden, in der n irgend eine ganze Zahl bezeichnet.

Entwickelt man, so erhalten alle Glieder mit Ausnahme des ersten, p^n , den Factor A ; man hat also:

$$(13) \quad P \equiv p^n \pmod{A}.$$

Denkt man sich zunächst n ungerade, so wird, wie leicht zu sehen, P

gerade oder ungerade sein, je nachdem p gerade oder ungerade ist. Für ein gerades p folgt aus §. 1:

$$p \equiv -1 \pmod{M}, \quad p \equiv 1 \pmod{N}$$

und also:

$$p^n \equiv -1 \pmod{M}, \quad p^n \equiv 1 \pmod{N},$$

oder wenn man die Congruenz (13) und die Gleichung $A = MN$ berücksichtigt:

$$P \equiv -1 \pmod{M}, \quad P \equiv 1 \pmod{N},$$

d. h. $P+1$ ist ein Vielfaches von M , und $P-1$ ein Vielfaches von N . Es muss also, da $P+1$ und $P-1$ relative Primzahlen sind und ihr Product durch $M'N' = MN$ theilbar ist, $M' = M$ und $N' = N$ sein. Die aus (10) folgende Gleichung ist also für diesen Fall $MR^2 - NS^2 = 2$, d. h. sie hat dieselben Coefficienten $M, -N, 2$, wie die aus (1) abgeleitete.

Ist p ungerade, so hat man nach §. 1:

$$p \equiv 1 \pmod{2M}, \quad p \equiv 1 \pmod{2N}$$

und folglich:

$$p^n \equiv -1 \pmod{2M}, \quad p^n \equiv 1 \pmod{2N}.$$

woraus sich mit Berücksichtigung der Congruenz (13) ergibt, dass $\frac{P+1}{2}$ ein Vielfaches von M und $\frac{P-1}{2}$ ein Vielfaches von N ist. Man schliesst dann wie vorher $M' = M, N' = N$, so dass die aus (10) abgeleitete Gleichung $MR^2 - NS^2 = 1$ dieselbe Form hat, wie die aus (1) folgende. Man sieht also, dass, wenn man von irgend einer Auflösung von (10) ausgeht, die einem ungeraden n entspricht, die sich ergebende Gleichung (11) oder (12) der Form nach mit der aus (1) abgeleiteten in (2) zusammenfällt. Es bliebe nun noch übrig, die einem geraden n entsprechenden Auflösungen von (10) zu betrachten. Allein, ohne uns bei diesem Falle aufzuhalten, bemerken wir nur, dass sich durch ähnliche Betrachtungen oder noch directer aus dem allgemeinen Ausdruck für P leicht zeigen lässt, dass man alsdann als abgeleitete Gleichung die folgende $R^2 - AS^2 = 1$ erhält, welche dieselbe Form wie (10) hat. Es ist somit bewiesen, dass in dem System von Gleichungen (2), wenn man darin M und N der Bedingung $A = MN$ unterwirft und unter r und s unbestimmte ganze Zahlen versteht, ausser der immer darin vorkommenden, $r^2 - As^2 = 1$, nur noch eine einzige Auflösung zulässt.

ÜBER EINE NEUE ANWENDUNG
BESTIMMTER INTEGRALE AUF DIE SUMMATION
ENDLICHER ODER UNENDLICHER REIHEN.

VON

G. LEJEUNE DIRICHLET.

Abhandlungen der Königlich Preussischen Akademie der Wissenschaften von 1835, S. 391—407.

ÜBER EINE NEUE ANWENDUNG BESTIMMTER INTEGRALE AUF DIE SUMMATION ENDLICHER ODER UNENDLICHER REIHEN.

[Gelesen in der Akademie der Wissenschaften am 25. Juni 1835.]

Unter den zahlreichen und überraschenden Folgerungen, welche GAUSS aus seiner Methode zur Auflösung der zweigliedrigen Gleichungen, oder wie man sie mit Rücksicht auf ihre geometrische Anwendung zu nennen pflegt, seiner Theorie der Kreistheilung gezogen hat, ist besonders die Bestimmung gewisser endlicher Reihen wegen der eigenthümlichen dabei zum Vorschein kommenden Schwierigkeiten merkwürdig. Bezeichnet man mit p irgend eine Primzahl und mit π wie gewöhnlich den halben Kreisumfang für den Radius 1, so lässt sich, je nachdem p die Form $4\mu+1$ oder die Form $4\mu+3$ hat, die Summe der Reihe:

$$\cos 0^2 \frac{2\pi}{p} + \cos 1^2 \frac{2\pi}{p} + \cos 2^2 \frac{2\pi}{p} + \dots + \cos (p-1)^2 \frac{2\pi}{p}$$

oder die der Reihe:

$$\sin 0^2 \frac{2\pi}{p} + \sin 1^2 \frac{2\pi}{p} + \sin 2^2 \frac{2\pi}{p} + \dots + \sin (p-1)^2 \frac{2\pi}{p}$$

auf eine höchst einfache Weise durch p ausdrücken. Die erwähnte Methode zeigt nämlich, dass diese Summe die Wurzel der reinen quadratischen Gleichung $x^2 = p$, und also $+\sqrt{p}$ oder $-\sqrt{p}$ ist. Da die Summe für jede Primzahl p nur einen Werth hat, so bleibt also bloss noch zu entscheiden, mit welchem Zeichen man die Wurzelgrösse zu nehmen habe. Eine Unbestimmtheit, wie die hier sich zeigende, findet sehr häufig statt, lässt sich aber gewöhnlich leicht beseitigen, indem aus der Natur der zu bestimmenden Grösse leicht erhellt, ob ihr das positive oder negative Zeichen zukommt. Im vorliegenden Falle aber treten dieser Entscheidung grosse Schwierigkeiten in den Weg, da die Glieder

der Reihe zum Theil positiv, zum Theil negativ sind, und sich im Allgemeinen nicht übersehen lässt, ob die einen oder die andern überwiegen. Für besondere Werthe von p ist die Frage natürlich, vermittelt der aus den Tafeln zu entnehmenden Werthe der trigonometrischen Functionen, leicht zu entscheiden, und man findet so, dass jedesmal das positive Zeichen genommen werden muss. Für die allgemeine Frage ist jedoch dadurch wenig gewonnen, und die Theorie der Kreistheilung scheint kein Mittel darzubieten, das auf dem Wege der Induction gefundene Resultat für alle Fälle festzustellen. GAUSS ist in seinen *Disquisitiones arithmeticae* auf die Bestimmung des Zeichens nicht eingegangen sondern hat dieselbe später zum Gegenstande einer besondern Abhandlung gemacht^{*)}. Das darin befolgte Verfahren, welches der Idee nach ebenso einfach als in der Ausführung scharfsinnig ist, besteht darin, die obigen Reihen oder vielmehr die allgemeinen Ausdrücke von derselben Form, in denen irgend eine ganze Zahl n an die Stelle der Primzahl p getreten ist, in ein Product von Sinus zu verwandeln, deren Bogen in arithmetischer Progression fortschreiten, nach welcher Umformung sich das Zeichen sogleich bestimmen lässt, indem man findet, dass die negativen Factoren in gerader Anzahl vorhanden sind. Die Schwierigkeit, a priori, d. h. vor Durchführung aller Rechnungen, klar zu übersehen, warum der von dem grossen Geometer eingeschlagene Weg zu einer so merkwürdigen Umformung führt, hat den Wunsch in mir erregt, die Frage auf eine andere vielleicht übersichtlichere Weise zu behandeln, und ich glaube, das Resultat meiner Bemühungen der Akademie vorlegen zu dürfen, da die Erfahrung vielfältig bewiesen hat, dass bei so schwierigen Untersuchungen Gewinn für die Wissenschaft daraus entspringen kann, wenn man dasselbe Problem unter sehr verschiedenen Gesichtspunkten betrachtet.

Eine neue Auflösung der oben erwähnten Aufgabe wird um so eher einiges Interesse darbieten können, als die schöne, von GAUSS gegebene Analyse bis jetzt die einzige ist, durch welche die eigenthümliche, durch das doppelte Zeichen hervorgebrachte Unbestimmtheit gehoben wird. Zwar hat sich auch LEBRIT mit der Summation dieser Reihen beschäftigt, allein seine Methode, wie scharfsinnig sie auch sei, scheint nicht geeignet, die eben bezeichnete Schwierigkeit zu heben, indem sie, wie die Kreistheilung, auf eine quadratische Gleichung

*) *Summatio quarundam serierum singularium.* Comment. recent. Societ. Gottg. Tom. I. 9)

9) Gauss' Werke, Band II, S. 9. — K.

chung führt. Zur Bestimmung des Zeichens ist der Verfasser genöthigt, die in ein Sinusproduct verwandelte Reihe zu Hülfe zu nehmen, ohne jedoch auf irgend eine Weise anzugeben, wie man sich von der Gleichheit dieser beiden Ausdrücke überzeugen könne*). Aber gerade in diesem Uebergange liegt, wie schon bemerkt worden, die eigentliche Schwierigkeit der Frage, und ist derselbe erst bewerkstelligt, so wird jede andere Betrachtung überflüssig, indem das Product, zu welchem man durch die Transformation gelangt, zu den längst bekannten gehört, welche schon EULER in seiner *Introductio in analysin infinitorum* auf eine höchst einfache Weise bestimmt hat.

§. 1.

Die in dieser Abhandlung enthaltenen Untersuchungen beruhen auf folgenden zwei Sätzen, auf welche man durch die Betrachtung der Reihen geführt wird, die nach den Sinus und Cosinus der Vielfachen einer Veränderlichen fortschreiten und für ein gewisses Intervall eine beliebig gegebene Function dieser Veränderlichen darstellen.

„Bezeichnet c eine Constante, welche die doppelte Bedingung $0 < c < \frac{\pi}{2}$ erfüllt, und ist $f(\beta)$ eine von $\beta = 0$ bis $\beta = c$ continuirlich bleibende Function von β , so nähert sich das Integral:

$$\int_0^c f(\beta) \frac{\sin(2k+1)\beta}{\sin\beta} d\beta$$

der Grenze $\frac{\pi}{2} f(0)$, wenn die darin enthaltene positive ganze Zahl k unendlich wird.“

„Sind b und c Constanten von solcher Beschaffenheit, dass $0 < b < c < \frac{\pi}{2}$, und bleibt die Function $f(\beta)$ continuirlich von $\beta = b$ bis $\beta = c$, so nähert sich das Integral:

$$\int_b^c f(\beta) \frac{\sin(2k+1)\beta}{\sin\beta} d\beta$$

bei unaufhörlichem Wachsen von k der Grenze Null.“

*) Journal für Mathematik von CRELLE, Band IX, S. 187.

In früheren Abhandlungen über die Theorie der vorher erwähnten Reihen *) habe ich gezeigt, wie sich diese beiden Sätze auf eine ebenso einfache als strenge Weise begründen lassen, wenn man zunächst annimmt, dass die Function $f(\beta)$ innerhalb der Grenzen der Integration, welcher sie unterworfen ist, nicht vom Abnehmen ins Zunehmen oder umgekehrt übergeht. Um von diesem besondern Falle zu dem allgemeineren überzugehen, wo die Function zwischen den Integrationsgrenzen eine beliebige Anzahl Maxima und Minima hat, braucht man nur die Integrale in andere zu zerlegen, deren Grenzen durch die Werthe von β gegeben werden, für welche ein Maximum oder Minimum stattfindet.

Um dies für den ersten Satz zu zeigen, so seien e_1, e_2, \dots, e_h der Grösse nach geordnet die zwischen 0 und c liegenden Werthe von β , welchen ein Maximum oder Minimum von $f(\beta)$ entspricht. Zerlegt man nun das Integral:

$$\int_0^c f(\beta) \frac{\sin(2k+1)\beta}{\sin\beta} d\beta$$

in $h+1$ andere, deren Grenzen 0 und e_1 , e_1 und e_2 , e_2 , \dots , e_h und c sind, so sind auf diese neuen Integrale die obigen für den erwähnten speciellen Fall als erwiesen vorausgesetzten Sätze anwendbar, und man sieht, dass alle diese Integrale mit Ausnahme des ersten für $k = \infty$ verschwinden, während das erste in demselben Falle den Werth $\frac{\pi}{2} f(0)$ annimmt, welcher Werth also auch die Grenze des Integrals:

$$\int_0^c f(\beta) \frac{\sin(2k+1)\beta}{\sin\beta} d\beta$$

für das unaufhörliche Wachsen von k ist. Auf ganz ähnliche Weise wird der Beweis des zweiten Satzes geführt.

Vermittelst der obigen Sätze ist es leicht, die Grenze des Integrals:

$$\int_0^c f(\beta) \frac{\sin(2k+1)\beta}{\sin\beta} d\beta$$

für $k = \infty$ zu bestimmen, wenn jetzt c irgend eine positive Constante bezeichnet. Bezeichnet $l\pi$ das grösste in c enthaltene Vielfache von π , so zerlege man das

*) Journal für Mathematik von CRELLE, Band IV, S. 157, oder Repertorium der Physik von DOVE und MOSER 5).

5) S. 117 und 133 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

vorige Integral in die beiden folgenden:

$$\int_0^{\pi} f(\beta) \frac{\sin(2k+1)\beta}{\sin\beta} d\beta, \quad \int_{\pi}^c f(\beta) \frac{\sin(2k+1)\beta}{\sin\beta} d\beta.$$

Das erste kann in $2l$ zwischen den Grenzen:

$$0 \text{ und } \frac{\pi}{2}, \quad \frac{\pi}{2} \text{ und } 2 \cdot \frac{\pi}{2}, \quad 2 \cdot \frac{\pi}{2} \text{ und } 3 \cdot \frac{\pi}{2}, \dots, (2l-1) \cdot \frac{\pi}{2} \text{ und } 2l \cdot \frac{\pi}{2}$$

genommene Integrale zerlegt werden, welche, wenn man der Reihe nach statt β in denselben:

$$\beta, \quad \pi-\beta, \quad \pi+\beta, \quad 2\pi-\beta, \quad \dots, \quad (l-1)\pi-\beta, \quad (l-1)\pi+\beta, \quad l\pi-\beta$$

schreibt und nachher auf das 2^{te} , 4^{te} , 6^{te} , ... die Gleichung

$$\int_{\sigma}^h \psi(\beta) d\beta = - \int_h^{\sigma} \psi(\beta) d\beta$$

angewendet, sich alle von $\beta = 0$ bis $\beta = \frac{\pi}{2}$ erstrecken. Sie können daher in ein Integral vereinigt werden, welches, da k eine ganze Zahl ist, offenbar die Form hat:

$$\int_0^{\frac{\pi}{2}} [f(\beta) + f(\pi-\beta) + f(\pi+\beta) + \dots + f((l-1)\pi-\beta) + f((l-1)\pi+\beta) + f(l\pi-\beta)] \frac{\sin(2k+1)\beta}{\sin\beta} d\beta$$

und nach dem ersten Satz für $k = \infty$ den Werth:

$$\pi \left(\frac{1}{2} f(0) + f(\pi) + \dots + f((l-1)\pi) + \frac{1}{2} f(l\pi) \right)$$

annimmt.

Was das andere Integral:

$$\int_{\pi}^c f(\beta) \frac{\sin(2k+1)\beta}{\sin\beta} d\beta$$

betrifft, so ist dasselbe Null, wenn $c = l\pi$ ist. Für alle andern Fälle bringe man dasselbe in die Form:

$$\int_0^{c-l\pi} f(l\pi+\beta) \frac{\sin(2k+1)\beta}{\sin\beta} d\beta.$$

indem man $l\pi+\beta$ für β setzt. Ist nun $c - l\pi$ nicht grösser als $\frac{\pi}{2}$, so folgt aus dem ersten Satz, dass sich das Integral für $k = \infty$ in $\frac{\pi}{2} f(l\pi)$ verwandelt.

Liegt hingegen $c - l\pi$ zwischen $\frac{\pi}{2}$ und π , so zerlege man es in zwei andere,

deren Grenzen 0 und $\frac{\pi}{2}$, $\frac{\pi}{2}$ und $c-l\pi$ sind. Das erste nimmt für $k = \infty$ den Werth $\frac{\pi}{2} f(l\pi)$ an, während das andere, welches dadurch, dass man $\pi - \beta$ für β schreibt, in:

$$\int_{(l+1)\pi - \beta}^{\pi} f((l+1)\pi - \beta) \frac{\sin(2k+1)\beta}{\sin\beta} d\beta$$

übergeht, nach dem zweiten Satz für $k = \infty$ verschwindet.

Fasst man das Vorhergehende zusammen, so ergibt sich, dass das Integral:

$$\int_0^c f(\beta) \frac{\sin(2k+1)\beta}{\sin\beta} d\beta,$$

wenn die darin enthaltene ganze positive Zahl k unaufhörlich wächst, sich immer der Grenze:

$$\pi(\frac{1}{2}f(0) + f(\pi) + \dots + f(l\pi)) = \frac{\pi}{2}f(0) + \pi \sum_{s=1}^{l-1} f(s\pi)$$

nähert, wo l das grösste in $\frac{c}{\pi}$ enthaltene Ganze bezeichnet, mit Ausnahme des einzigen Falles, wo c ein Vielfaches von π ist, in welchem Falle das letzte Glied $\pi f(l\pi)$ der vorigen Summe nur halb zu nehmen ist.

§. 2.

Man betrachte die beiden Integrale:

$$\int_{-\infty}^{+\infty} \cos(\alpha^2) d\alpha = a, \quad \int_{-\infty}^{+\infty} \sin(\alpha^2) d\alpha = b^*).$$

*) Man behauptet zuweilen, dass Integrale, welche zwischen den Grenzen $-\infty$ und ∞ genommen sind, nothwendig immer unbestimmt werden, wenn die Function unter dem Zeichen an diesen Grenzen nicht verschwindet. Die hier betrachteten Integrale erfüllen diese Bedingung nicht und haben dennoch ganz bestimmte Werthe, wie sogleich erhellt, wenn man sie in die Form:

$$\int_0^{\infty} \frac{\cos\beta}{\sqrt{\beta}} d\beta, \quad \int_0^{\infty} \frac{\sin\beta}{\sqrt{\beta}} d\beta$$

bringt. Jedes der Integrale:

$$\int_{-p}^p \cos(\alpha^2) d\alpha, \quad \int_{-p}^p \sin(\alpha^2) d\alpha$$

nähert sich also einer bestimmten Grenze, wenn man die positive Grösse p ins Unendliche wachsen lässt, mag nun dieses Wachsen continuirlich oder, wie im Folgenden, nach irgend einem beliebigen Gesetze sprungweise geschehen.

Obgleich schon seit EULER bekannt ist, dass die Constanten a und b beide den Werth $\sqrt{\frac{\pi}{2}}$ haben, so brauchen wir dies nicht vorauszusetzen, da sich diese Werthe aus unserer Analyse von selbst ergeben.

Setzt man:

$$a = \frac{\beta}{2} \sqrt{\frac{n}{2\pi}}.$$

wo β eine neue Veränderliche und n eine positive ganze Zahl bezeichnet, so erhält man:

$$\int_{-\infty}^{+\infty} \cos \frac{n\beta^2}{8\pi} d\beta = 2a \sqrt{\frac{2\pi}{n}} \cdot \int_{-\infty}^{+\infty} \sin \frac{n\beta^2}{8\pi} d\beta = 2b \sqrt{\frac{2\pi}{n}}.$$

Wir denken uns diese beiden Integrale zunächst von $-(2k+1)\pi$ bis $(2k+1)\pi$ genommen, wo k eine positive ganze Zahl bezeichnet, und setzen nachher $k = \infty$. Zerlegt man jedes der beiden Integrale in $2k+1$ neue, deren Grenzen:

$$-(2k+1)\pi \quad \text{und} \quad -(2k-1)\pi, \quad -(2k-1)\pi \quad \text{und} \quad -(2k-3)\pi, \quad \dots \\ \dots \quad (2k-3)\pi \quad \text{und} \quad (2k-1)\pi, \quad (2k-1)\pi \quad \text{und} \quad (2k+1)\pi$$

sind, und schreibt in diesen neuen Integralen der Reihe nach statt β :

$$-2k\pi + \gamma, \quad -2(k-1)\pi + \gamma, \quad \dots, \quad 2(k-1)\pi + \gamma, \quad 2k\pi + \gamma,$$

so erhalten alle die Grenzen $-\pi$ und $+\pi$, und man findet:

$$\int_{-\pi}^{+\pi} d\gamma \sum_{h=-k}^{h=k} \cos \frac{n}{8\pi} (\gamma + 2h\pi)^2, \quad \int_{-\pi}^{+\pi} d\gamma \sum_{h=-k}^{h=k} \sin \frac{n}{8\pi} (\gamma + 2h\pi)^2.$$

Die Zahl n kann eine der folgenden vier Formen: 4μ , $4\mu+1$, $4\mu+2$, $4\mu+3$ haben. Findet zunächst die erste statt, d. h. ist n durch 4 theilbar, so kann man $\frac{n}{2} h^2 \pi$ als ein Vielfaches von 2π unter dem trigonometrischen Zeichen weglassen, und man hat:

$$\sum_{h=-k}^{h=k} \cos \frac{n}{8\pi} (\gamma + 2h\pi)^2 = \sum_{h=-k}^{h=k} \cos \left(\frac{n\gamma^2}{8\pi} + \frac{h n \gamma}{2} \right),$$

wofür man auch schreiben kann, indem man die Glieder, die entgegengesetzten Werthen von h entsprechen, vereinigt und sich einer bekannten Summationsformel bedient:

$$\begin{aligned} \cos \frac{n\gamma^2}{8\pi} + \sum_{h=1}^{h=k} \left[\cos \left(\frac{n\gamma^2}{8\pi} + \frac{hn\gamma}{2} \right) + \cos \left(\frac{n\gamma^2}{8\pi} - \frac{hn\gamma}{2} \right) \right] \\ = \left(1 + 2 \sum_{h=1}^{h=k} \cos \frac{hn\gamma}{2} \right) \cos \frac{n\gamma^2}{8\pi} = \cos \frac{n\gamma^2}{8\pi} \frac{\sin(2k+1) \frac{n\gamma}{4}}{\sin \frac{n\gamma}{4}}. \end{aligned}$$

Man findet auf dieselbe Weise für die im zweiten Integral enthaltene Summe:

$$\sin \frac{n\gamma^2}{8\pi} \frac{\sin(2k+1) \frac{n\gamma}{4}}{\sin \frac{n\gamma}{4}}.$$

Setzt man diese Werthe ein und führt eine neue durch die Gleichung $\frac{n\gamma}{4} = \beta$ bestimmte Veränderliche β ein, so erhalten die Integrale die Form:

$$\frac{4}{n} \int_{-\frac{n\pi}{4}}^{\frac{n\pi}{4}} \cos \left(\frac{2\beta^2}{n\pi} \right) \frac{\sin(2k+1)\beta}{\sin\beta} d\beta, \quad \frac{4}{n} \int_{-\frac{n\pi}{4}}^{\frac{n\pi}{4}} \sin \left(\frac{2\beta^2}{n\pi} \right) \frac{\sin(2k+1)\beta}{\sin\beta} d\beta.$$

Da die Functionen unter dem Integralzeichen für β und $-\beta$ denselben Werth haben, so kann man auch von $\beta = 0$ bis $\beta = \frac{n\pi}{4}$ integriren und die Resultate doppelt nehmen. Man erhält so:

$$\frac{8}{n} \int_0^{\frac{n\pi}{4}} \cos \left(\frac{2\beta^2}{n\pi} \right) \frac{\sin(2k+1)\beta}{\sin\beta} d\beta, \quad \frac{8}{n} \int_0^{\frac{n\pi}{4}} \sin \left(\frac{2\beta^2}{n\pi} \right) \frac{\sin(2k+1)\beta}{\sin\beta} d\beta.$$

Nach Obigem werden diese Ausdrücke für $k = \infty$ respective:

$$2a \sqrt{\frac{2\pi}{n}}, \quad 2b \sqrt{\frac{2\pi}{n}}.$$

Andrerseits ergeben sich aber auch die der Annahme $k = \infty$ entsprechenden Werthe unmittelbar aus dem am Ende des vorigen Paragraphen aufgestellten Satze, bei dessen Anwendung man nicht übersehen darf, dass der dort erwähnte Ausnahmefall hier stattfindet, indem $\frac{n}{4}$ eine ganze Zahl ist. Man gelangt so durch Vergleichung zu den Resultaten:

$$\begin{aligned} \frac{1}{2} + \cos 1^2 \frac{2\pi}{n} + \cos 2^2 \frac{2\pi}{n} + \dots + \cos \left(\frac{n}{4} - 1 \right)^2 \frac{2\pi}{n} + \frac{1}{2} \cos \left(\frac{n}{4} \right)^2 \frac{2\pi}{n} &= \frac{a}{2} \sqrt{\frac{2\pi}{n}}, \\ \sin 1^2 \frac{2\pi}{n} + \sin 2^2 \frac{2\pi}{n} + \dots + \sin \left(\frac{n}{4} - 1 \right)^2 \frac{2\pi}{n} + \frac{1}{2} \sin \left(\frac{n}{4} \right)^2 \frac{2\pi}{n} &= \frac{b}{2} \sqrt{\frac{2\pi}{n}}. \end{aligned}$$

Giebt man, um die Constanten a , b zu bestimmen, n einen besondern Werth, z. B. 4, so kommt:

$$\frac{1}{2} + \frac{1}{2} \cos \frac{\pi}{2} = \frac{a}{2} \sqrt{\frac{2}{\pi}}, \quad \frac{1}{2} \sin \frac{\pi}{2} = \frac{b}{2} \sqrt{\frac{2}{\pi}}$$

und folglich:

$$a = \sqrt{\frac{\pi}{2}}, \quad b = \sqrt{\frac{\pi}{2}}.$$

Setzt man diesen Werth für a in die erste Gleichung und transformirt die Glieder derselben, mit Ausnahme des ersten und letzten, nach der aus der Voraussetzung $n = 4\mu$ evidenten Formel:

$$\cos s^2 \frac{2\pi}{n} = \frac{1}{2} \cos s^2 \frac{2\pi}{n} + \frac{1}{2} \cos \left(\frac{n}{2} - s \right)^2 \frac{2\pi}{n}.$$

so wird dieselbe:

$$1 + \cos 1^2 \frac{2\pi}{n} + \cos 2^2 \frac{2\pi}{n} + \dots + \cos \left(\frac{n}{2} - 1 \right)^2 \frac{2\pi}{n} = \frac{1}{2} \sqrt{n}.$$

oder wenn man $\frac{1}{2} + \frac{1}{2} \cos \left(\frac{n}{2} \right)^2 \frac{2\pi}{n}$ für das erste Glied 1 schreibt und die übrigen mit Hülfe der Gleichung:

$$\cos s^2 \frac{2\pi}{n} = \frac{1}{2} \cos s^2 \frac{2\pi}{n} + \frac{1}{2} \cos (n-s)^2 \frac{2\pi}{n}$$

umformt:

$$1 + \cos 1^2 \frac{2\pi}{n} + \cos 2^2 \frac{2\pi}{n} + \dots + \cos (n-1)^2 \frac{2\pi}{n} = \sqrt{n}.$$

Ganz auf dieselbe Weise folgt aus der zweiten der oben erhaltenen Gleichungen:

$$\sin 1^2 \frac{2\pi}{n} + \sin 2^2 \frac{2\pi}{n} + \dots + \sin (n-1)^2 \frac{2\pi}{n} = \sqrt{n}.$$

§. 3.

Die Fälle, wo n nicht durch 4 theilbar sondern in einer der Formen $4\mu + 1$, $4\mu + 2$, $4\mu + 3$ enthalten ist, lassen sich in ähnlicher Weise behandeln. Da jedoch die Resultate nicht unmittelbar in ihrer einfachsten Gestalt erscheinen, so wenden wir uns zu einem etwas modificirten Verfahren, welches allgemeinere Resultate liefert.

Setzt man in der vorher erhaltenen Gleichung:

$$\int_{-x}^{+x} \cos(a^2) da = \sqrt{\frac{\pi}{2}}$$

$a = \beta + g$, wo β eine neue Veränderliche und g eine reelle Constante bezeichnet, so erhält man:

$$\int_{-x}^{+x} \cos(\beta + g)^2 d\beta = \sqrt{\frac{\pi}{2}},$$

oder wenn man entwickelt:

$$\int_{-x}^{+x} \cos(\beta^2 + g^2) \cos 2g\beta d\beta - \int_{-x}^{+x} \sin(\beta^2 + g^2) \sin 2g\beta d\beta = \sqrt{\frac{\pi}{2}}.$$

Das zweite Integral ist offenbar Null, und die Gleichung lässt sich in folgende Form bringen:

$$\cos(g^2) \int_{-x}^{+x} \cos(\beta^2) \cos 2g\beta d\beta - \sin(g^2) \int_{-x}^{+x} \sin(\beta^2) \cos 2g\beta d\beta = \sqrt{\frac{\pi}{2}}.$$

Aus der Gleichung:

$$\int_{-x}^{+x} \sin(a^2) da = \sqrt{\frac{\pi}{2}}$$

folgt auf dieselbe Weise:

$$\sin(g^2) \int_{-x}^{+x} \cos(\beta^2) \cos 2g\beta d\beta + \cos(g^2) \int_{-x}^{+x} \sin(\beta^2) \cos 2g\beta d\beta = \sqrt{\frac{\pi}{2}},$$

und durch Combination mit dem vorigen Resultat erhält man sogleich die bekannten Gleichungen:

$$\int_{-x}^{+x} \cos(\beta^2) \cos 2g\beta d\beta = \sqrt{\frac{\pi}{2}} (\cos(g^2) + \sin(g^2)),$$

$$\int_{-x}^{+x} \sin(\beta^2) \cos 2g\beta d\beta = \sqrt{\frac{\pi}{2}} (\cos(g^2) - \sin(g^2)).$$

Setzt man:

$$\beta = \frac{a}{2} \sqrt{\frac{n}{2\pi}} \quad \text{und} \quad g = i \sqrt{\frac{2\pi}{n}},$$

wo a eine neue Veränderliche und n , i positive Constanten bezeichnen, die im

Folgenden als ganze Zahlen gelten sollen, so kommt:

$$\int_{-\pi}^{\pi} \cos\left(\frac{n\alpha^2}{8\pi}\right) \cos i\alpha d\alpha = \frac{2\pi}{\sqrt{n}} \left(\cos \frac{2i^2\pi}{n} + \sin \frac{2i^2\pi}{n} \right),$$

$$\int_{-\pi}^{\pi} \sin\left(\frac{n\alpha^2}{8\pi}\right) \cos i\alpha d\alpha = \frac{2\pi}{\sqrt{n}} \left(\cos \frac{2i^2\pi}{n} - \sin \frac{2i^2\pi}{n} \right).$$

Es sei jetzt:

$$(1) \quad F(\alpha) = b_0 + b_1 \cos \alpha + b_2 \cos 2\alpha + \dots = \sum b_i \cos i\alpha$$

eine beliebige endliche oder unendliche Reihe, deren Coefficienten von α unabhängig sind. Es soll im letzteren Falle nur vorausgesetzt werden, dass die Reihe convergirt und die Function von α , welche sie darstellt, continuirlich ist.

Multiplieirt man die vorigen Gleichungen mit b_i und summirt von $i = 0$ bis zu derselben Grenze wie in (1), so erhält man:

$$(2) \quad \begin{cases} \int_{-\pi}^{\pi} \cos \frac{n\alpha^2}{8\pi} F(\alpha) d\alpha = \frac{2\pi}{\sqrt{n}} \sum b_i \left(\cos \frac{2i^2\pi}{n} + \sin \frac{2i^2\pi}{n} \right) = \frac{2\pi}{\sqrt{n}} (G + H), \\ \int_{-\pi}^{\pi} \sin \frac{n\alpha^2}{8\pi} F(\alpha) d\alpha = \frac{2\pi}{\sqrt{n}} \sum b_i \left(\cos \frac{2i^2\pi}{n} - \sin \frac{2i^2\pi}{n} \right) = \frac{2\pi}{\sqrt{n}} (G - H), \end{cases}$$

wenn man zur Abkürzung:

$$\sum b_i \cos \frac{2i^2\pi}{n} = G \quad \text{und} \quad \sum b_i \sin \frac{2i^2\pi}{n} = H$$

setzt. Um diese beiden Integrale zu finden, denken wir uns dieselben zunächst von $-(4k+1)\pi$ bis $(4k+1)\pi$, wo k eine positive ganze Zahl bezeichnet, genommen, und lassen nachher k unendlich werden. Zerlegt man jedes dieser Integrale in $4k+1$ andere, deren Grenzen durch die beiden Ausdrücke $(2h-1)\pi$ und $(2h+1)\pi$ gegeben werden, wenn man h alle ganzen Werthe von $-2k$ bis $2k$ incl. beilegt, und führt in diese Integrale eine für jedes durch die Gleichung $\alpha = \gamma + 2h\pi$ bestimmte neue Veränderliche γ ein, so werden die Grenzen für alle $-\pi$ und $+\pi$, und man erhält mit Berücksichtigung, dass nach (1) offenbar $F(\gamma + 2h\pi) = F(\gamma)$ ist:

$$\int_{-\pi}^{+\pi} d\gamma F(\gamma) \sum \cos \frac{n}{8\pi} (\gamma + 2h\pi)^2, \quad \int_{-\pi}^{+\pi} d\gamma F(\gamma) \sum \sin \frac{n}{8\pi} (\gamma + 2h\pi)^2,$$

wo sich die Summationen von $h = -2k$ bis $h = 2k$ erstrecken. Vereinigt man die Glieder, welche entgegengesetzten Werthen von h entsprechen, so er-

hält man für die im ersten Integral enthaltene Summe:

$$\begin{aligned} \cos \frac{n\gamma^2}{8\pi} + \sum_{h=1}^{h=2k} \left(\cos \frac{n}{8\pi} (\gamma + 2h\pi)^2 + \cos \frac{n}{8\pi} (\gamma - 2h\pi)^2 \right) \\ = \cos \frac{n\gamma^2}{8\pi} + 2 \sum_{h=1}^{h=2k} \cos \frac{n}{8\pi} (\gamma^2 + 4h^2\pi^2) \cos \frac{hn\gamma}{2}. \end{aligned}$$

Der Factor:

$$\cos \frac{n}{8\pi} (\gamma^2 + 4h^2\pi^2) \quad \text{oder} \quad \cos \left(nh^2 \frac{\pi}{2} + \frac{n\gamma^2}{8\pi} \right)$$

unter dem Summenzeichen hat nur zwei verschiedene Werthe und ist offenbar:

$$\cos \frac{n\gamma^2}{8\pi} \quad \text{oder} \quad \cos \left(\frac{n\pi}{2} + \frac{n\gamma^2}{8\pi} \right).$$

je nachdem h gerade oder ungerade ist. Trennt man daher die Glieder, die einem geraden h entsprechen, von denen, welche zu einem ungeraden h gehören, so findet man:

$$\begin{aligned} \cos \frac{n\gamma^2}{8\pi} (1 + 2 \cos n\gamma + 2 \cos 2n\gamma + \dots + 2 \cos kn\gamma) \\ + \cos \left(\frac{n\pi}{2} + \frac{n\gamma^2}{8\pi} \right) \left(2 \cos \frac{n\gamma}{2} + 2 \cos \frac{3n\gamma}{2} + \dots + 2 \cos (2k-1) \frac{n\gamma}{2} \right), \end{aligned}$$

oder wenn man für die beiden Reihen ihre bekannten Werthe:

$$\frac{\sin(2k+1) \frac{n\gamma}{2}}{\sin \frac{n\gamma}{2}}, \quad \frac{\sin(4k+1) \frac{n\gamma}{4}}{\sin \frac{n\gamma}{4}}, \quad \frac{\sin(2k+1) \frac{n\gamma}{2}}{\sin \frac{n\gamma}{2}}$$

substituiert:

$$\frac{\sin(4k+1) \frac{n\gamma}{4}}{\sin \frac{n\gamma}{4}} \cos \left(\frac{n\pi}{2} + \frac{n\gamma^2}{8\pi} \right) + \frac{\sin(2k+1) \frac{n\gamma}{2}}{\sin \frac{n\gamma}{2}} \left(\cos \frac{n\gamma^2}{8\pi} - \cos \left(\frac{n\pi}{2} + \frac{n\gamma^2}{8\pi} \right) \right).$$

Ganz auf dieselbe Weise ergibt sich für die im zweiten Integrale enthaltene Summe der Werth:

$$\frac{\sin(4k+1) \frac{n\gamma}{4}}{\sin \frac{n\gamma}{4}} \sin \left(\frac{n\pi}{2} + \frac{n\gamma^2}{8\pi} \right) + \frac{\sin(2k+1) \frac{n\gamma}{2}}{\sin \frac{n\gamma}{2}} \left(\sin \frac{n\gamma^2}{8\pi} - \sin \left(\frac{n\pi}{2} + \frac{n\gamma^2}{8\pi} \right) \right).$$

Die vorhergehenden Ausdrücke bleiben ungeändert, wenn γ in $-\gamma$ verwandelt wird; dasselbe gilt nach (1) von $F(\gamma)$. Man kann daher die Integrale von $\gamma = 0$

bis $\gamma = \pi$ nehmen und den Factor 2 vorsetzen. Man erhält so:

$$2 \int_0^{\frac{\pi}{2}} \frac{\sin(4k+1)\frac{n\gamma}{4}}{\sin \frac{n\gamma}{4}} \cos\left(\frac{n\pi}{2} + \frac{n\gamma^2}{8\pi}\right) F(\gamma) d\gamma + 2 \int_0^{\frac{\pi}{2}} \frac{\sin(2k+1)\frac{n\gamma}{2}}{\sin \frac{n\gamma}{2}} \left(\cos \frac{n\gamma^2}{8\pi} - \cos\left(\frac{n\pi}{2} + \frac{n\gamma^2}{8\pi}\right)\right) F(\gamma) d\gamma.$$

$$2 \int_0^{\frac{\pi}{2}} \frac{\sin(4k+1)\frac{n\gamma}{4}}{\sin \frac{n\gamma}{4}} \sin\left(\frac{n\pi}{2} + \frac{n\gamma^2}{8\pi}\right) F(\gamma) d\gamma + 2 \int_0^{\frac{\pi}{2}} \frac{\sin(2k+1)\frac{n\gamma}{2}}{\sin \frac{n\gamma}{2}} \left(\sin \frac{n\gamma^2}{8\pi} - \sin\left(\frac{n\pi}{2} + \frac{n\gamma^2}{8\pi}\right)\right) F(\gamma) d\gamma.$$

Setzt man im ersten und dritten Integral $\beta = \frac{n\gamma}{4}$, im zweiten und vierten $\beta = \frac{n\gamma}{2}$, so gehen diese beiden Ausdrücke über in:

$$\frac{8}{n} \int_0^{\frac{n\pi}{4}} \frac{\sin(4k+1)\beta}{\sin \beta} \cos\left(\frac{n\pi}{2} + \frac{2\beta^2}{n\pi}\right) F\left(\frac{4\beta}{n}\right) d\beta + 4 \int_0^{\frac{n\pi}{2}} \frac{\sin(2k+1)\beta}{\sin \beta} \left(\cos \frac{\beta^2}{2n\pi} - \cos\left(\frac{n\pi}{2} + \frac{\beta^2}{2n\pi}\right)\right) F\left(\frac{2\beta}{n}\right) d\beta,$$

$$\frac{8}{n} \int_0^{\frac{n\pi}{4}} \frac{\sin(4k+1)\beta}{\sin \beta} \sin\left(\frac{n\pi}{2} + \frac{2\beta^2}{n\pi}\right) F\left(\frac{4\beta}{n}\right) d\beta + 4 \int_0^{\frac{n\pi}{2}} \frac{\sin(2k+1)\beta}{\sin \beta} \left(\sin \frac{\beta^2}{2n\pi} - \sin\left(\frac{n\pi}{2} + \frac{\beta^2}{2n\pi}\right)\right) F\left(\frac{2\beta}{n}\right) d\beta.$$

Die Grenzen, welchen sich diese Ausdrücke nähern, wenn die darin enthaltene ganze Zahl k wachsend gedacht wird, ergeben sich auf der Stelle aus dem im ersten Paragraphen bewiesenen Satze. Man hat daher, wenn man, wie früher, die in (2) enthaltenen Reihen zur Abkürzung mit G und H bezeichnet und auf beiden Seiten mit $\sqrt{\frac{n}{2\pi}}$ multiplicirt:

$$G+H = \frac{1}{\sqrt{n}} \left(1 + \cos \frac{n\pi}{2}\right) F(0) + \frac{4}{\sqrt{n}} \sum \cos\left(\frac{n\pi}{2} + \frac{2s^2\pi}{n}\right) F\left(\frac{4s\pi}{n}\right) + \frac{2}{\sqrt{n}} \sum \left(\cos \frac{s^2\pi}{2n} - \cos\left(\frac{n\pi}{2} + \frac{s^2\pi}{2n}\right)\right) F\left(\frac{2s\pi}{n}\right),$$

$$G-H = \frac{1}{\sqrt{n}} \sin \frac{n\pi}{2} F(0) + \frac{4}{\sqrt{n}} \sum \sin\left(\frac{n\pi}{2} + \frac{2s^2\pi}{n}\right) F\left(\frac{4s\pi}{n}\right) + \frac{2}{\sqrt{n}} \sum \left(\sin \frac{s^2\pi}{2n} - \sin\left(\frac{n\pi}{2} + \frac{s^2\pi}{2n}\right)\right) F\left(\frac{2s\pi}{n}\right).$$

Von den beiden in jeder dieser Gleichungen enthaltenen Summationen erstreckt sich die erste von $s = 1$ bis zu der grössten in $\frac{n}{4}$, die zweite von $s = 1$ bis zu der grössten in $\frac{n}{2}$ enthaltenen ganzen Zahl, und es ist zugleich

zu bemerken, dass das letzte Glied der zweiten Summe nur halb zu nehmen ist, wenn $\frac{n}{2}$ ein Ganzes ist, und dasselbe gilt vom letzten Gliede der ersten, wenn auch $\frac{n}{4}$ ein Ganzes ist.

Die eben gefundenen Gleichungen, welche die Bestimmung der endlichen oder unendlichen Reihen G und H auf die von andern endlichen Reihen zurückführen, enthalten als specielle Fälle die in der Einleitung erwähnten Summationen. Reducirt man nämlich die Reihe (1) auf n Glieder und setzt alle ihre Coefficienten der Einheit gleich, so ist:

$$F(\alpha) = 1 + \cos \alpha + \cos 2\alpha + \dots + \cos(n-1)\alpha = \frac{1}{2} + \frac{1}{2} \frac{\sin(2n-1)\frac{\alpha}{2}}{\sin \frac{\alpha}{2}},$$

und man hat offenbar $F\left(\frac{2t\pi}{n}\right) = 0$, für jede nicht durch n theilbare ganze Zahl t . Alle Glieder der obigen Summen verschwinden daher durch die Factoren $F\left(\frac{4s\pi}{n}\right)$, $F\left(\frac{2s\pi}{n}\right)$, und da $F(0) = n$ ist, so kommt ganz einfach:

$$G + H = \left(1 + \cos \frac{n\pi}{2}\right) \sqrt{n}, \quad G - H = \sin \frac{n\pi}{2} \sqrt{n}$$

und folglich:

$$G = \frac{1}{2} \left(1 + \cos \frac{n\pi}{2} + \sin \frac{n\pi}{2}\right) \sqrt{n}, \quad H = \frac{1}{2} \left(1 + \cos \frac{n\pi}{2} - \sin \frac{n\pi}{2}\right) \sqrt{n}.$$

Legt man der ganzen Zahl n nach einander die 4 Formen 4μ , $4\mu+1$, $4\mu+2$, $4\mu+3$ bei und führt die durch G und H bezeichneten Reihen wieder ein, so erhält man:

$$\sum \cos \frac{2i^2\pi}{n} = \sqrt{n}, \quad \sum \sin \frac{2i^2\pi}{n} = \sqrt{n}, \quad n = 4\mu,$$

$$\sum \cos \frac{2i^2\pi}{n} = \sqrt{n}, \quad \sum \sin \frac{2i^2\pi}{n} = 0, \quad n = 4\mu+1,$$

$$\sum \cos \frac{2i^2\pi}{n} = 0, \quad \sum \sin \frac{2i^2\pi}{n} = 0, \quad n = 4\mu+2,$$

$$\sum \cos \frac{2i^2\pi}{n} = 0, \quad \sum \sin \frac{2i^2\pi}{n} = \sqrt{n}, \quad n = 4\mu+3,$$

wo sich die Summationen von $i = 0$ bis $i = n-1$ erstrecken.

§. 4.

Zum Schluss wollen wir nach GAUSS noch zeigen, wie man aus den eben erhaltenen Summenausdrücken den Fundamentalsatz der Theorie der quadratischen Reste auf eine höchst einfache Weise ableiten kann.

Bezeichnet p eine ungerade Primzahl, so ist der Rest irgend eines nicht durch p theilbaren Quadrats bei der Division durch p offenbar unter denen enthalten, welche die Reihe $1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2$ liefert, und man beweist leicht, dass diese Reste, welche in irgend einer Ordnung mit:

$$(I.) \quad a_1, a_2, a_3, \dots, a_{\frac{p-1}{2}}$$

bezeichnet werden sollen, alle von einander verschieden sind. Es seien ferner:

$$(II.) \quad b_1, b_2, b_3, \dots, b_{\frac{p-1}{2}}$$

diejenigen Zahlen der Reihe $1, 2, 3, \dots, p-1$, welche in (I.) nicht vorkommen. Dies vorausgesetzt, sagt man bekanntlich von einer durch p nicht theilbaren Zahl q , sie sei quadratischer Rest oder Nichtrest von p , je nachdem der Rest, den q bei der Division durch p lässt, zu (I.) oder zu (II.) gehört, und man beweist ohne Schwierigkeit, dass, je nachdem der erste oder der zweite Fall stattfindet, die Reste von $1^2q, 2^2q, 3^2q, \dots, \left(\frac{p-1}{2}\right)^2q$, wenn man von der Ordnung absieht, mit (I.) oder (II.) zusammenfallen*).

Man betrachte die Summe:

$$M = \sum_{s=0}^{s=\frac{p-1}{2}} e^{s^2 \frac{2q^2}{p}} \sqrt{-1}.$$

wo e wie gewöhnlich die Basis der natürlichen Logarithmen bezeichnet. Trennt man das Glied, welches $s=0$ entspricht, von den übrigen, und vereinigt diese paarweise mit Berücksichtigung der evidenten Gleichung:

$$e^{s^2 \frac{2q^2}{p}} \sqrt{-1} = e^{(p-s)^2 \frac{2q^2}{p}} \sqrt{-1},$$

so kommt:

$$M = 1 + 2 \sum_{s=1}^{s=\frac{p-1}{2}} e^{s^2 \frac{2q^2}{p}} \sqrt{-1},$$

oder wenn man statt der Zahlen $1^2q, 2^2q, \dots, \left(\frac{p-1}{2}\right)^2q$ die Reste setzt,

* Disquisitiones arithmeticae. Sect. IV.

welche sie bei der Division durch p lassen, welche Veränderung keine andere Folge hat als die, dass man im Exponenten Vielfache von $2\pi\sqrt{-1}$ weglässt, so erhält man:

$$M = 1 + 2 \sum_{s=1}^{\frac{p-1}{2}} \rho^{\alpha_s} p^{\frac{2\pi}{p} V^{-1}}, \quad \text{oder} \quad M = 1 + 2 \sum_{s=1}^{\frac{p-1}{2}} \rho^{\beta_s} p^{\frac{2\pi}{p} V^{-1}},$$

je nachdem nämlich q quadratischer Rest oder Nichtrest von p ist. Da offenbar:

$$\sum_{s=1}^{\frac{p-1}{2}} \rho^{\alpha_s} p^{\frac{2\pi}{p} V^{-1}} + \sum_{s=1}^{\frac{p-1}{2}} \rho^{\beta_s} p^{\frac{2\pi}{p} V^{-1}} = \sum_{s=1}^{p-1} \rho^s p^{\frac{2\pi}{p} V^{-1}} = -1$$

ist, so lässt sich die im letztern Falle stattfindende Gleichung auch so schreiben:

$$M = -1 - 2 \sum_{s=1}^{\frac{p-1}{2}} \rho^{\alpha_s} p^{\frac{2\pi}{p} V^{-1}}.$$

Beide Fälle sind daher in der Gleichung:

$$\sum_{s=1}^{\frac{p-1}{2}} \rho^{\alpha_s} p^{\frac{2\pi}{p} V^{-1}} = \delta (1 + 2 \sum_{s=1}^{\frac{p-1}{2}} \rho^{\alpha_s} p^{\frac{2\pi}{p} V^{-1}})$$

vereinigt, wenn man unter δ die positiv oder negativ genommene Einheit versteht, je nachdem q quadratischer Rest oder Nichtrest von p ist. Die Gleichung gilt für jede nicht durch p theilbare Zahl q ; um den von q unabhängigen, zwischen den Klammern enthaltenen Ausdruck zu erhalten, setze man $q = 1$; es ist alsdann $\delta = 1$ und folglich:

$$\sum_{s=1}^{\frac{p-1}{2}} \rho^{\alpha_s} p^{\frac{2\pi}{p} V^{-1}} = 1 + 2 \sum_{s=1}^{\frac{p-1}{2}} \rho^{\alpha_s} p^{\frac{2\pi}{p} V^{-1}}.$$

Der Werth der ersten Seite ergibt sich sogleich aus den Ausdrücken des vorigen Paragraphen und ist, da p ungerade, $1/p$ oder $Vp\sqrt{-1}$, je nachdem p die Form $4\mu+1$ oder die Form $4\mu+3$ hat. Beide Werthe sind in dem Ausdrucke $Vp(\sqrt{-1})^{\binom{p-1}{2}}$ enthalten, und es ist also:

$$1 + 2 \sum_{s=1}^{\frac{p-1}{2}} \rho^{\alpha_s} p^{\frac{2\pi}{p} V^{-1}} = Vp(\sqrt{-1})^{\binom{p-1}{2}}.$$

Die obige Gleichung wird so:

$$\sum_{s=0}^{s=q-1} e^{\frac{2\pi s}{p}} V^{-1} = \delta V p (V^{-1})^{\left(\frac{p-1}{2}\right)^2}.$$

Nimmt man jetzt an, q sei ebenfalls eine ungerade Primzahl, so erhält man durch eine blosse Vertauschung:

$$\sum_{t=0}^{t=q-1} e^{\frac{2\pi t}{q}} V^{-1} = \varepsilon V q (V^{-1})^{\left(\frac{q-1}{2}\right)^2},$$

wo $\varepsilon = +1$ oder -1 , je nachdem p quadratischer Rest oder Nichtrest von q ist. Werden beide Gleichungen in einander multiplicirt, so kommt:

$$\sum_{s=0}^{s=q-1} \sum_{t=0}^{t=p-1} e^{\frac{2\pi (qs+pt)}{pq}} V^{-1} = \delta \varepsilon V p q (V^{-1})^{\left(\frac{p-1}{2}\right)^2 + \left(\frac{q-1}{2}\right)^2},$$

oder was ganz dasselbe ist, indem man $4st\pi V^{-1}$ zum Exponenten von e addirt:

$$\sum_{s=0}^{s=q-1} \sum_{t=0}^{t=p-1} e^{\frac{2\pi (qs+pt)}{pq}} V^{-1} = \delta \varepsilon V p q (V^{-1})^{\left(\frac{p-1}{2}\right)^2 + \left(\frac{q-1}{2}\right)^2}.$$

Der Ausdruck $qs+pt$ lässt offenbar bei der Division durch pq innerhalb der Summationsgrenzen nicht zweimal denselben Rest; wären nämlich die Reste, welche $qs+pt$ und $qs'+pt'$ entsprechen, einander gleich, so wäre $q(s-s') + p(t-t')$ durch pq und folglich, da p und q von einander verschiedene Primzahlen bezeichnen, $s-s'$ durch p , und $t-t'$ durch q theilbar, was wegen der Grenzen, in welche $s, s',$ sowie t, t' eingeschlossen sind, nur stattfinden kann, wenn zugleich $s = s'$ und $t = t'$ ist. Die Reste von $qs+pt$ in Bezug auf den Divisor pq sind also $0, 1, 2, 3, \dots, pq-1$, und man kann diese Reste an die Stelle der Werthe setzen, welche $qs+pt$ bei der doppelten Summation successive annimmt, indem durch diese Veränderung bloss Vielfache von $2\pi V^{-1}$ im Exponenten weggeworfen werden. Man erhält so:

$$\sum_{s=0}^{s=pq-1} e^{\frac{2\pi s}{pq}} V^{-1} = \delta \varepsilon V p q (V^{-1})^{\left(\frac{p-1}{2}\right)^2 + \left(\frac{q-1}{2}\right)^2},$$

oder wenn man für die erste Seite ihren aus dem vorigen Paragraphen sich ergebenden Werth $V p q (V^{-1})^{\left(\frac{pq-1}{2}\right)^2}$ setzt und den gemeinschaftlichen Factor $V p q$ weglässt:

$$\delta \varepsilon = (V^{-1})^{\left(\frac{pq-1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2 - \left(\frac{q-1}{2}\right)^2}.$$

Der Exponent von $\sqrt{-1}$ lässt sich in die Form:

$$\frac{1}{2}(p-1)(q-1) + (p-1)(q-1) \left(\frac{(p+1)}{2} \cdot \frac{(q+1)}{2} - 1 \right)$$

bringen, wo der zweite Theil als durch 4 theilbar weggelassen werden kann.

Es ist also:

$$\delta \varepsilon = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.$$

Diese Gleichung enthält das oben erwähnte Reciprocitätsgesetz: denn es folgt aus derselben, dass, wenn p und q beide die Form $4\mu + 3$ haben, $\delta = -\varepsilon$, in allen andern Fällen aber $\delta = \varepsilon$ ist.

SUR L'USAGE DES INTÉGRALES DÉFINIES
DANS LA SOMMATION DES SÉRIES
FINIES OU INFINIES.

PAR

M. G. LEJEUNE DIRICHLET.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 17 p. 57—67.

SUR L'USAGE DES INTÉGRALES DÉFINIES DANS LA SOMMATION DES SÉRIES FINIES OU INFINIES.

[Lu à l'Académie des Sciences de Berlin le 25 Juin 1835.]

(Extrait.)

Parmi les conséquences nombreuses et inattendues que M. GAUSS a tirées de sa belle théorie des équations binômes, il y en a une qui présente une singularité très remarquable. La lettre p désignant un nombre premier $4m+1$, et q un nombre premier $4m+3$, il résulte de cette théorie que les deux expressions:

$$s = \sum_{i=0}^{i=p-1} \cos \frac{2i^2\pi}{p} \quad . \quad t = \sum_{i=0}^{i=q-1} \sin \frac{2i^2\pi}{q}$$

sont données par ces deux équations du second degré: $s^2 = p$, $t^2 = q$. On conclut de là $s = \pm \sqrt{p}$, $t = \pm \sqrt{q}$, où il ne s'agit plus que de fixer le signe qui doit être unique dans l'un et l'autre cas, les sommes précédentes étant complètement déterminées. En attribuant des valeurs particulières aux nombres p et q , on trouve toujours que c'est le signe supérieur qui doit avoir lieu, mais il est très difficile de prouver la généralité de ce résultat indiqué par l'induction. Dans ses „*Disquisitiones arithmeticae*“ M. GAUSS ne s'était pas attaché à lever cette difficulté singulière, mais il y est revenu dans un Mémoire particulier*) que les géomètres regardent comme une des plus belles productions de ce profond analyste. La méthode dont il y fait usage, consiste à transformer les sommes précédentes, ou plutôt les expressions plus générales qui s'en déduisent, en y remplaçant les nombres premiers p et q par un entier quelconque n , en produits de sinus d'ares équidifférents, produits qui sont très faciles à évaluer et qui ne présentent plus aucune ambigüité de signe. La difficulté de se rendre bien compte à quoi tient le succès des considérations délicates par

*) Summatio quarundam serierum singularium. Comment. recent. societ. Gotting. Tom. I.)

) Gauss Werke, Band II, S. 9. K.

lesquelles l'illustre auteur opère cette ingénieuse transformation, n'ayant fait rechercher, si on ne pourrait pas résoudre la même question sans y recourir, je suis parvenu au théorème suivant qui comprend les sommations précédentes :

„La somme de la série finie ou infinie :

$$F(a) = c_0 + c_1 \cos a + c_2 \cos 2a + \dots$$

étant connue, on peut toujours exprimer, au moyen de la fonction $F(a)$, les nouvelles séries :

$$c_0 + c_1 \cos 1^2 \cdot \frac{2\pi}{n} + c_2 \cos 2^2 \cdot \frac{2\pi}{n} + \dots,$$

$$c_1 \sin 1^2 \cdot \frac{2\pi}{n} + c_2 \sin 2^2 \cdot \frac{2\pi}{n} + \dots,$$

qui ont les mêmes coefficients que la précédente.”

Je me flatte que cette nouvelle manière de parvenir aux résultats si remarquables de M. GAUSS pourra avoir quelque intérêt, l'histoire de la théorie des nombres nous montrant par de nombreux exemples, que c'est surtout dans cette partie de la science qu'il y a de l'avantage à envisager la même question sous des points de vue très différents. La méthode de M. GAUSS était jusqu'à présent le seul moyen de vaincre la difficulté indiquée et qui consiste dans l'ambiguïté du signe. Celle que M. LIBRI a donnée, quoique très ingénieuse, ne paraît pas propre à résoudre cette difficulté puisqu'elle fait dépendre les sommes cherchées d'une équation du second degré. Pour faire disparaître l'ambiguïté que cette circonstance fait naître*), le savant auteur a recours à l'expression transformée en produit, sans indiquer aucun moyen de parvenir à cette transformée. Mais ce passage de la somme au produit est à lui seul la question tout entière, puisqu'une fois effectué, il dispense de toute autre analyse, l'expression en produit étant du nombre de ceux qu'ETTLER a déterminés depuis longtemps par les considérations les plus simples.

§. 1.

L'analyse dont nous ferons usage, repose sur ces deux théorèmes :

„La constante c remplissant la double condition $0 < c < \frac{1}{2}\pi$, et la fonction $f(\beta)$ étant continue depuis $\beta = 0$ jusqu'à $\beta = c$, l'intégrale

* Voyez le tome IX du Journal de CHÉLLE, p. 187.

$\int_0^{\frac{1}{2}\pi} \frac{\sin(2k+1)\beta}{\sin\beta} f(\beta) d\beta$ convergera vers la limite $\frac{1}{2}\pi f'(0)$ pour des valeurs indéfiniment croissantes de l'entier positif k .*

„Les constantes b et c étant telles qu'on ait $0 < b < c < \frac{1}{2}\pi$, et la fonction $f(\beta)$ étant supposée continue depuis $\beta = b$ jusqu'à $\beta = c$, l'intégrale $\int_b^c \frac{\sin(2k+1)\beta}{\sin\beta} f(\beta) d\beta$ convergera dans la même circonstance vers la limite zéro.“

Ces théorèmes se démontrent facilement, comme je l'ai fait voir dans un précédent Mémoire[†]), lorsqu'on suppose d'abord la fonction $f(\beta)$ toujours croissante, ou toujours décroissante entre les limites de l'intégration. Pour passer ensuite au cas général où cette fonction présente plusieurs maxima et minima entre ces limites, il suffit de décomposer les intégrales en d'autres entre les limites desquelles la fonction $f(\beta)$ n'est plus alternativement croissante et décroissante.

Au moyen de ces théorèmes on détermine facilement la limite vers laquelle converge l'intégrale:

$$\int_0^a \frac{\sin(2k+1)\beta}{\sin\beta} f(\beta) d\beta,$$

a désignant une constante positive quelconque, et la fonction $f(\beta)$ étant continue depuis $\beta = 0$ jusqu'à $\beta = a$. Soit $l\pi$ le plus grand multiple de π contenu dans a , l'intégrale précédente sera la somme de celles-ci:

$$\int_0^{l\pi} \frac{\sin(2k+1)\beta}{\sin\beta} f(\beta) d\beta, \quad \int_{l\pi}^a \frac{\sin(2k+1)\beta}{\sin\beta} f(\beta) d\beta.$$

La première étant décomposée en $2l$ autres prises entre les limites:

$$0 \text{ et } \frac{1}{2}\pi, \quad \frac{1}{2}\pi \text{ et } 2 \cdot \frac{1}{2}\pi, \quad 2 \cdot \frac{1}{2}\pi \text{ et } 3 \cdot \frac{1}{2}\pi, \quad \dots, \quad (2l-1) \cdot \frac{1}{2}\pi \text{ et } 2l \cdot \frac{1}{2}\pi,$$

si dans ces nouvelles intégrales l'on écrit au lieu de β :

$$\beta, \quad \pi - \beta, \quad \pi + \beta, \quad 2\pi - \beta, \quad \dots, \quad l\pi - \beta,$$

et si l'on transforme ensuite les intégrales dont le rang est un nombre pair,

* Voyez le Journal de CRELLE tome IV p. 157 ou le „Repertorium der Physik von DOVE und MOSER“, où la même démonstration est simplifiée à quelques égards.¹⁾

¹⁾ 8. 117 und 133 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

d'après la formule :

$$\int_y^x \psi(\beta) d\beta = - \int_h^y \psi(\beta) d\beta.$$

toutes ces intégrales s'étendront depuis $\beta = 0$ jusqu'à $\beta = \frac{1}{2}\pi$. En les réunissant donc et ayant égard à ce que k est un entier, il viendra :

$$\int_0^{\frac{1}{2}\pi} [f(\beta) + f(\pi - \beta) + f(\pi + \beta) + \dots + f((l-1)\pi + \beta) + f(l\pi - \beta)] \frac{\sin(2k+1)\beta}{\sin\beta} d\beta.$$

expression qui, d'après le premier des théorèmes précédents, convergera pour des valeurs croissantes de k vers cette limite :

$$\pi(\frac{1}{2}f(0) + f(\pi) + f(2\pi) + \dots + \frac{1}{2}f(l\pi)).$$

La seconde intégrale :

$$\int_{-\pi}^a \frac{\sin(2k+1)\beta}{\sin\beta} f(\beta) d\beta,$$

évidemment nulle lorsque $a = l\pi$, devient généralement :

$$\int_0^{a-l\pi} \frac{\sin(2k+1)\beta}{\sin\beta} f(l\pi + \beta) d\beta,$$

en y remplaçant β par $l\pi + \beta$. Lorsque $a - l\pi$ ne surpasse pas $\frac{1}{2}\pi$, il résulte du premier théorème qu'elle converge vers la limite $\frac{1}{2}\pi f(l\pi)$: dans le cas où $a - l\pi$ est compris entre $\frac{1}{2}\pi$ et π , on décomposera l'intégrale précédente en deux autres prises l'une depuis $\beta = 0$ jusqu'à $\beta = \frac{1}{2}\pi$, l'autre depuis $\beta = \frac{1}{2}\pi$ jusqu'à $\beta = a - l\pi$. La première deviendra toujours $\frac{1}{2}\pi f(l\pi)$ pour $k = \infty$, tandis que la seconde qui, par le changement de β en $\pi - \beta$, prend la forme :

$$\int_{(l+1)\pi - a}^{\frac{1}{2}\pi} \frac{\sin(2k+1)\beta}{\sin\beta} f((l+1)\pi - \beta) d\beta,$$

converge vers la limite zéro en vertu du second théorème.

En réunissant ce qui précède, on voit que l'intégrale :

$$\int_0^a \frac{\sin(2k+1)\beta}{\sin\beta} f(\beta) d\beta,$$

lorsque l'entier positif k qu'elle renferme devient infini, prend toujours cette valeur :

$$\pi(\frac{1}{2}f(0) + f(\pi) + f(2\pi) + \dots + f(l\pi)) = \frac{1}{2}\pi f(0) + \pi \sum_{s=1}^{l-1} f(s\pi).$$

$l\pi$ désignant le plus grand multiple de π contenu dans a . Il n'y a d'exception que lorsque a est un multiple exact de π , le dernier terme $\pi f(l\pi)$ devant, dans ce cas, être réduit à la moitié de sa valeur.

§. 2.

Considérons les deux intégrales:

$$\int_{-\infty}^{+\infty} \cos(u^2) du = a, \quad \int_{-\infty}^{+\infty} \sin(u^2) du = b^*.$$

Quoiqu'on sache qu'on a $a = \sqrt{\frac{1}{2}}\pi$, $b = \sqrt{\frac{1}{2}}\pi$, nous n'avons pas besoin de supposer connues les valeurs de ces deux constantes qui se présentent d'elles-mêmes dans l'analyse que nous allons développer. Si l'on pose dans la première intégrale $u = \beta + g$, β désignant une nouvelle variable et g étant une constante réelle quelconque, il viendra:

$$\int_{-\infty}^{+\infty} \cos(\beta+g)^2 d\beta = \int_{-\infty}^{+\infty} \cos(\beta^2+g^2) \cos 2g\beta \cdot d\beta - \int_{-\infty}^{+\infty} \sin(\beta^2+g^2) \sin 2g\beta \cdot d\beta = a.$$

La seconde intégrale étant évidemment nulle, cette équation prendra la forme:

$$\cos(g^2) \int_{-\infty}^{+\infty} \cos(\beta^2) \cos 2g\beta \cdot d\beta - \sin(g^2) \int_{-\infty}^{+\infty} \sin(\beta^2) \cos 2g\beta \cdot d\beta = a.$$

On trouve d'une manière toute semblable:

$$\sin(g^2) \int_{-\infty}^{+\infty} \cos(\beta^2) \cos 2g\beta \cdot d\beta + \cos(g^2) \int_{-\infty}^{+\infty} \sin(\beta^2) \cos 2g\beta \cdot d\beta = b.$$

En éliminant successivement chacune de ces deux intégrales, on aura ces équations connues:

$$\begin{aligned} \int_{-\infty}^{+\infty} \cos(\beta^2) \cos 2g\beta \cdot d\beta &= a \cos(g^2) + b \sin(g^2), \\ \int_{-\infty}^{+\infty} \sin(\beta^2) \cos 2g\beta \cdot d\beta &= b \cos(g^2) - a \sin(g^2). \end{aligned}$$

*) Il n'est peut-être pas inutile de prévenir une difficulté que l'emploi de ces deux intégrales pourrait faire naître. Quelques auteurs ont énoncé qu'une intégrale prise entre des limites infinies devient nécessairement indéterminée, lorsque la fonction sous le signe ne s'évanouit pas à ces deux limites. Les intégrales que nous considérons ne satisfont pas à cette condition et sont néanmoins complètement déterminées, comme on le voit sur le champ en les mettant sous cette autre forme:

$$\int_0^{+\infty} \frac{\cos \beta}{\sqrt{\beta}} d\beta, \quad \int_0^{+\infty} \frac{\sin \beta}{\sqrt{\beta}} d\beta.$$

Il résulte de là que les intégrales $\int \cos(\alpha^2) d\alpha$, $\int \sin(\alpha^2) d\alpha$, prises depuis $\alpha = -p$ jusqu'à $\alpha = p$, convergent l'une et l'autre vers une limite fixe, lorsque la quantité positive p croît indéfiniment, soit que cette augmentation se fasse d'une manière continue, soit qu'elle ait lieu, comme dans ce qui va suivre, par sauts et suivant une loi quelconque. Il n'en serait pas de même pour l'intégrale $\int \cos u du$, qu'on suppose quelquefois égale à zéro, et qui est essentiellement indéterminée, du moins tant qu'on la considère en elle-même.

Si l'on pose:

$$\beta = \frac{1}{2}a \left| \frac{n}{2\pi} \right., \quad g = i \left| \frac{2\pi}{n} \right.$$

a étant une nouvelle variable, et n et i désignant des constantes positives que l'on considérera comme des entiers dans ce qui va suivre, il viendra:

$$\int_{-\infty}^{+\infty} \cos\left(\frac{na^2}{8\pi}\right) \cos ia da = 2 \left| \frac{2\pi}{n} \right. \cdot \left(a \cos \frac{2i^2\pi}{n} + b \sin \frac{2i^2\pi}{n} \right),$$

$$\int_{-\infty}^{+\infty} \sin\left(\frac{na^2}{8\pi}\right) \cos ia da = 2 \left| \frac{2\pi}{n} \right. \cdot \left(b \cos \frac{2i^2\pi}{n} - a \sin \frac{2i^2\pi}{n} \right).$$

Cela posé, soit:

$$(1) \quad F(a) = e_n + c_1 \cos a + c_2 \cos 2a + \dots = \sum e_i \cos ia$$

une série de cosinus finie ou infinie. On suppose seulement que lorsque la série se prolonge à l'infini, elle est convergente et exprime une fonction continue de a . Les équations précédentes étant multipliées par e_i , si l'on somme ensuite entre les mêmes limites que dans l'équation (1), on aura:

$$(2) \quad \begin{cases} \int_{-\infty}^{+\infty} \cos \frac{na^2}{8\pi} F(a) da = 2 \left| \frac{2\pi}{n} \right. (aG + bH), \\ \int_{-\infty}^{+\infty} \sin \frac{na^2}{8\pi} F(a) da = 2 \left| \frac{2\pi}{n} \right. (bG - aH), \end{cases}$$

où j'ai fait pour abrégier:

$$(3) \quad \sum e_i \cos \frac{2i^2\pi}{n} = G, \quad \sum e_i \sin \frac{2i^2\pi}{n} = H.$$

Pour obtenir les intégrales précédentes, on les supposera d'abord prises depuis $a = -(4k+1)\pi$ jusqu'à $a = (4k+1)\pi$, k désignant un nombre entier positif quelconque que l'on considérera ensuite comme infini. Chacune de ces deux intégrales étant décomposée en $4k+1$ nouvelles intégrales dont les limites résultent des expressions $(2h-1)\pi$ et $(2h+1)\pi$, en attribuant à h toutes les valeurs entières depuis $h = -2k$ jusqu'à $h = 2k$, si l'on pose ensuite $\beta = 2h\pi + \gamma$ dans chacune de ces nouvelles intégrales, en observant qu'on a, d'après l'équation (1), $F(2h\pi + \gamma) = F(\gamma)$, il viendra:

$$\int_{-\pi}^{+\pi} d\gamma F(\gamma) \sum \cos \frac{n}{8\pi} (\gamma + 2h\pi)^2, \quad \int_{-\pi}^{+\pi} d\gamma F(\gamma) \sum \sin \frac{n}{8\pi} (\gamma + 2h\pi)^2.$$

les sommations s'étendant depuis $h = -2k$ jusqu'à $h = 2k$. En réunissant les termes de la première somme qui correspondent à des valeurs opposées de h , cette somme prendra cette autre forme :

$$\begin{aligned} \cos \frac{n\gamma^2}{8\pi} + \sum_{h=1}^{h=2k} \left(\cos \frac{n}{8\pi} (\gamma + 2h\pi)^2 + \cos \frac{n}{8\pi} (\gamma - 2h\pi)^2 \right) \\ = \cos \frac{n\gamma^2}{8\pi} + 2 \sum_{h=1}^{h=2k} \cos \frac{n}{8\pi} (\gamma^2 + 4h^2\pi^2) \cos \frac{hn\gamma}{2}. \end{aligned}$$

Le facteur $\cos \frac{n}{8\pi} (\gamma^2 + 4h^2\pi^2)$ n'a évidemment que deux valeurs différentes, à savoir :

$$\cos \left(\frac{n\gamma^2}{8\pi} \right) \quad \text{ou} \quad \cos \left(\frac{n\gamma^2}{8\pi} + \frac{n\pi}{2} \right),$$

selon que h est pair ou impair, puisque h^2 , dans le premier cas, a la forme 4μ et, dans le second, celle-ci : $4\mu + 1$. Il viendra donc en réunissant séparément les termes pour lesquels h est pair et ceux où h est impair :

$$\begin{aligned} \cos \frac{n\gamma^2}{8\pi} (1 + 2\cos n\gamma + 2\cos 2n\gamma + \dots + 2\cos kn\gamma) \\ + \cos \left(\frac{1}{2}n\pi + \frac{n\gamma^2}{8\pi} \right) [2\cos \frac{1}{2}n\gamma + 2\cos 3(\frac{1}{2}n\gamma) + \dots + 2\cos(2k-1)(\frac{1}{2}n\gamma)]. \end{aligned}$$

En substituant pour ces deux séries les expressions connues :

$$\frac{\sin(2k+1)\frac{1}{2}n\gamma}{\sin \frac{1}{2}n\gamma}, \quad \frac{\sin(4k+1)\frac{1}{4}n\gamma}{\sin \frac{1}{4}n\gamma} - \frac{\sin(2k+1)\frac{1}{2}n\gamma}{\sin \frac{1}{2}n\gamma}.$$

il viendra :

$$\frac{\sin(4k+1)\frac{1}{4}n\gamma}{\sin \frac{1}{4}n\gamma} \cos \left(\frac{1}{2}n\pi + \frac{n\gamma^2}{8\pi} \right) + \frac{\sin(2k+1)\frac{1}{2}n\gamma}{\sin \frac{1}{2}n\gamma} \left[\cos \frac{n\gamma^2}{8\pi} - \cos \left(\frac{1}{2}n\pi + \frac{n\gamma^2}{8\pi} \right) \right].$$

La somme que la seconde intégrale renferme, est pareillement :

$$\frac{\sin(4k+1)\frac{1}{4}n\gamma}{\sin \frac{1}{4}n\gamma} \cdot \sin \left(\frac{1}{2}n\pi + \frac{n\gamma^2}{8\pi} \right) + \frac{\sin(2k+1)\frac{1}{2}n\gamma}{\sin \frac{1}{2}n\gamma} \left[\sin \frac{n\gamma^2}{8\pi} - \sin \left(\frac{1}{2}n\pi + \frac{n\gamma^2}{8\pi} \right) \right].$$

Ces expressions ayant la même valeur pour γ et pour $-\gamma$, et la même circonstance ayant lieu pour $F(\gamma)$ en vertu de l'équation (1), il est permis de n'étendre les intégrations que depuis $\gamma = 0$ jusqu'à $\gamma = \pi$, et de doubler les résultats. On trouve ainsi ces deux expressions :

$$\begin{aligned}
& 2 \int_0^{\pi} \frac{\sin(4k+1)\frac{1}{4}n\gamma}{\sin\frac{1}{4}n\gamma} \cos\left(\frac{1}{2}n\pi + \frac{n\gamma^2}{8\pi}\right) F(\gamma) d\gamma \\
& + 2 \int_0^{\pi} \frac{\sin(2k+1)\frac{1}{2}n\gamma}{\sin\frac{1}{2}n\gamma} \left[\cos \frac{n\gamma^2}{8\pi} - \cos\left(\frac{1}{2}n\pi + \frac{n\gamma^2}{8\pi}\right) \right] F(\gamma) d\gamma, \\
& 2 \int_0^{\pi} \frac{\sin(4k+1)\frac{1}{4}n\gamma}{\sin\frac{1}{4}n\gamma} \sin\left(\frac{1}{2}n\pi + \frac{n\gamma^2}{8\pi}\right) F(\gamma) d\gamma \\
& + 2 \int_0^{\pi} \frac{\sin(2k+1)\frac{1}{2}n\gamma}{\sin\frac{1}{2}n\gamma} \left[\sin \frac{n\gamma^2}{8\pi} - \sin\left(\frac{1}{2}n\pi + \frac{n\gamma^2}{8\pi}\right) \right] F(\gamma) d\gamma.
\end{aligned}$$

Si l'on pose $\frac{1}{4}n\gamma = \beta$ dans la première et dans la troisième intégrale, et $\frac{1}{2}n\gamma = \beta$ dans la seconde et la quatrième, ces expressions prennent la forme:

$$\begin{aligned}
& \frac{8}{n} \int_0^{\frac{n\pi}{4}} \frac{\sin(4k+1)\beta}{\sin\beta} \cos\left(\frac{1}{2}n\pi + \frac{2\beta^2}{n\pi}\right) F\left(\frac{4\beta}{n}\right) d\beta \\
& + \frac{4}{n} \int_0^{\frac{n\pi}{2}} \frac{\sin(2k+1)\beta}{\sin\beta} \left[\cos \frac{\beta^2}{2n\pi} - \cos\left(\frac{1}{2}n\pi + \frac{\beta^2}{2n\pi}\right) \right] F\left(\frac{2\beta}{n}\right) d\beta, \\
& \frac{8}{n} \int_0^{\frac{n\pi}{4}} \frac{\sin(4k+1)\beta}{\sin\beta} \sin\left(\frac{1}{2}n\pi + \frac{2\beta^2}{n\pi}\right) F\left(\frac{4\beta}{n}\right) d\beta \\
& + \frac{4}{n} \int_0^{\frac{n\pi}{2}} \frac{\sin(2k+1)\beta}{\sin\beta} \left[\sin \frac{\beta^2}{2n\pi} - \sin\left(\frac{1}{2}n\pi + \frac{\beta^2}{2n\pi}\right) \right] F\left(\frac{2\beta}{n}\right) d\beta.
\end{aligned}$$

Les limites de ces expressions correspondant à $k = \infty$ résultent immédiatement du théorème énoncé à la fin du premier paragraphe: en substituant ces valeurs dans les équations (2) et multipliant par $\frac{1}{2} \sqrt{\frac{n}{2\pi}}$, il viendra:

$$\begin{aligned}
aG + bH &= \sqrt{\frac{\pi}{2n}} \cdot \left(1 + \cos \frac{n\pi}{2}\right) F(0) + 4 \sqrt{\frac{\pi}{2n}} \cdot \Sigma \cos\left(\frac{n\pi}{2} + \frac{2s^2\pi}{n}\right) F\left(\frac{4s\pi}{n}\right) \\
&+ 2 \sqrt{\frac{\pi}{2n}} \cdot \Sigma \left[\cos \frac{s^2\pi}{2n} - \cos\left(\frac{n\pi}{2} + \frac{s^2\pi}{2n}\right) \right] F\left(\frac{2s\pi}{n}\right), \\
bG - aH &= \sqrt{\frac{\pi}{2n}} \cdot \sin \frac{n\pi}{2} F(0) + 4 \sqrt{\frac{\pi}{2n}} \cdot \Sigma \sin\left(\frac{n\pi}{2} + \frac{2s^2\pi}{n}\right) F\left(\frac{4s\pi}{n}\right) \\
&+ 2 \sqrt{\frac{\pi}{2n}} \cdot \Sigma \left[\sin \frac{s^2\pi}{2n} - \sin\left(\frac{n\pi}{2} + \frac{s^2\pi}{2n}\right) \right] F\left(\frac{2s\pi}{n}\right).
\end{aligned}$$

Dans chacune de ces deux équations la première somme s'étend depuis $s = 1$ jusqu'au plus grand entier contenu dans $\frac{1}{4}n$, la seconde depuis $s = 1$, jusqu'au

plus grand entier contenu dans $\frac{1}{2}n$, le dernier terme de la seconde somme devant être réduit à moitié lorsque $\frac{1}{2}n$ est un nombre entier, et la même chose ayant lieu pour la première lorsque $\frac{1}{2}n$ est aussi un entier.

Pour déduire de ces équations les sommations dont il a été question dans le préambule de ce Mémoire, supposons la série (1) composée de n termes et tous ses coefficients égaux à l'unité. On aura alors :

$$F(\alpha) = 1 + \cos\alpha + \cos 2\alpha + \dots + \cos(n-1)\alpha = \frac{1}{2} + \frac{\sin(n-\frac{1}{2})\alpha}{2\sin\frac{1}{2}\alpha},$$

et la fonction $F\left(\frac{2t\pi}{n}\right)$ sera évidemment nulle, lorsque t est un nombre entier non-divisible par n . Il résulte de là, en ayant égard aux limites des sommations précédentes, que tous leurs termes disparaissent, et comme on a aussi $F(0) = n$, il viendra simplement :

$$aG + bH = (1 + \cos\frac{1}{2}n\pi) \cdot \sqrt{\frac{1}{2}n\pi}, \quad bG - aH = \sin\frac{1}{2}n\pi \cdot \sqrt{\frac{1}{2}n\pi}.$$

Pour déterminer les deux quantités a et b , indépendantes de n , il suffira de donner à n une valeur particulière. Posant par exemple $n = 1$, on aura $G = 1$, $H = 0$, et les équations précédentes deviendront $a = \sqrt{\frac{1}{2}\pi}$, $b = \sqrt{\frac{1}{2}\pi}$. On a donc généralement, quel que soit n :

$$G + H = (1 + \cos\frac{1}{2}n\pi) \cdot \sqrt{n}, \quad G - H = \sin\frac{1}{2}n\pi \cdot \sqrt{n},$$

et par conséquent :

$$G = \frac{1}{2}(1 + \cos\frac{1}{2}n\pi + \sin\frac{1}{2}n\pi)\sqrt{n}, \quad H = \frac{1}{2}(1 + \cos\frac{1}{2}n\pi - \sin\frac{1}{2}n\pi)\sqrt{n}.$$

En attribuant successivement à n ces 4 formes : 4μ , $4\mu + 1$, $4\mu + 2$, $4\mu + 3$, et remettant pour G et H les séries que ces lettres représentent d'après les équations (3), on aura :

$$\begin{aligned} \Sigma \cos \frac{2i^2\pi}{n} &= \sqrt{n}, & \Sigma \sin \frac{2i^2\pi}{n} &= \sqrt{n}, & n &= 4\mu, \\ \Sigma \cos \frac{2i^2\pi}{n} &= \sqrt{n}, & \Sigma \sin \frac{2i^2\pi}{n} &= 0, & n &= 4\mu + 1, \\ \Sigma \cos \frac{2i^2\pi}{n} &= 0, & \Sigma \sin \frac{2i^2\pi}{n} &= 0, & n &= 4\mu + 2, \\ \Sigma \cos \frac{2i^2\pi}{n} &= 0, & \Sigma \sin \frac{2i^2\pi}{n} &= \sqrt{n}, & n &= 4\mu + 3, \end{aligned}$$

les sommations s'étendant depuis $i = 0$ jusqu'à $i = n - 1$.

§. 3.

Je ne terminerai pas cet extrait, sans avoir rappelé les considérations extrêmement simples par lesquelles M. GAUSS, dans le Mémoire déjà cité, a déduit des expressions précédentes, la loi de réciprocité qui existe entre deux nombres premiers impairs quelconques.

Le nombre premier impair p étant considéré comme diviseur, le reste provenant d'un carré quelconque non-divisible par p , sera évidemment compris parmi ceux que donne la série:

$$1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2$$

et l'on prouve facilement que ces restes que je désignerai par:

$$(I) \quad a_1, a_2, a_3, \dots, a_{\frac{p-1}{2}}$$

pris dans un ordre quelconque, sont tous différents entre eux. Soient encore:

$$(II) \quad b_1, b_2, b_3, \dots, b_{\frac{p-1}{2}}$$

ceux des nombres 1, 2, 3, ..., $p-1$ que la série (I) ne renferme pas. Cela posé, le nombre quelconque q non-divisible par p , est dit résidu ou non-résidu quadratique par rapport au diviseur p , selon que le reste de q appartient à la série (I) ou à la série (II), et l'on s'assure facilement que les restes de:

$$1^2 \cdot q, 2^2 \cdot q, 3^2 \cdot q, \dots, \left(\frac{p-1}{2}\right)^2 q,$$

abstraction faite de l'ordre, coïncident avec (I) ou (II), selon que le premier ou le second de ces deux cas a lieu*).

Considérons la somme $\sum_{s=0}^{s=p-1} e^{\frac{2\pi}{p} s^2} V^{-1}$, dans laquelle e désigne à l'ordinaire la base des logarithmes népériens. Comme p est impair, il résulte des expressions du paragraphe précédent que cette somme est Vp ou $Vp \cdot V^{-1}$ selon que p a la forme $4\mu+1$ ou celle-ci: $4\mu+3$. Cette double valeur étant donnée par la formule unique $Vp(V-1)^{\left(\frac{p-1}{2}\right)^2}$, ou aura:

$$\sum_{s=0}^{s=p-1} e^{\frac{2\pi}{p} s^2} V^{-1} = Vp(V-1)^{\left(\frac{p-1}{2}\right)^2}.$$

Si l'on met à part le premier terme et que l'on réunisse deux à deux les termes correspondant à s et à $p-s$, en ayant égard à l'équation évidente:

$$e^{\frac{2\pi}{p} s^2} V^{-1} = e^{\frac{2\pi}{p} (p-s)^2} V^{-1}.$$

*) Disquisitiones arithmeticae. Sect. IV.

il viendra :

$$1 + 2 \sum_{s=1}^{s=\frac{p-1}{2}} e^{s^2 \cdot \frac{2\pi}{p}} \sqrt{-1} = \sqrt{p} (\sqrt{-1})^{\left(\frac{p-1}{2}\right)^2},$$

ou ce qui revient au même, en rejetant les multiples de $2\pi\sqrt{-1}$ dans l'exposant :

$$1 + 2 \sum_{s=1}^{s=\frac{p-1}{2}} e^{a_s \cdot \frac{2\pi}{p}} \sqrt{-1} = \sqrt{p} (\sqrt{-1})^{\left(\frac{p-1}{2}\right)^2}.$$

On a pareillement :

$$P = \sum_{s=0}^{s=p-1} e^{s^2 \cdot \frac{2q\pi}{p}} \sqrt{-1} = 1 + 2 \sum_{s=1}^{s=\frac{p-1}{2}} e^{s^2 \cdot \frac{2q\pi}{p}} \sqrt{-1},$$

et comme les restes de la série $1^2 \cdot q, 2^2 \cdot q, 3^2 \cdot q, \dots, \left(\frac{p-1}{2}\right)^2 \cdot q$, coïncident avec (I) ou (II), selon que q est ou n'est pas résidu quadratique par rapport à p , on a respectivement dans ces deux cas, en négligeant toujours les multiples de $2\pi\sqrt{-1}$ dans l'exposant :

$$P = 1 + 2 \sum_{s=1}^{s=\frac{p-1}{2}} e^{a_s \cdot \frac{2\pi}{p}} \sqrt{-1} \quad \text{ou} \quad P = 1 + 2 \sum_{s=1}^{s=\frac{p-1}{2}} e^{b_s \cdot \frac{2\pi}{p}} \sqrt{-1},$$

expressions dont la seconde, en vertu de l'équation évidente :

$$\sum_{s=1}^{s=\frac{p-1}{2}} e^{a_s \cdot \frac{2\pi}{p}} \sqrt{-1} + \sum_{s=1}^{s=\frac{p-1}{2}} e^{b_s \cdot \frac{2\pi}{p}} \sqrt{-1} = \sum_{s=1}^{s=p-1} e^{s \cdot \frac{2\pi}{p}} \sqrt{-1} = -1,$$

se change en :

$$P = -1 - 2 \sum_{s=1}^{s=\frac{p-1}{2}} e^{a_s \cdot \frac{2\pi}{p}} \sqrt{-1}.$$

Si donc l'on désigne par δ l'unité prise positivement ou négativement selon que q est ou n'est pas résidu quadratique par rapport à p , on aura l'équation qui comprend les deux cas :

$$\sum_{s=0}^{s=p-1} e^{s^2 \cdot \frac{2q\pi}{p}} \sqrt{-1} = \delta \left(1 + 2 \sum_{s=1}^{s=\frac{p-1}{2}} e^{a_s \cdot \frac{2\pi}{p}} \sqrt{-1} \right) = \delta \sqrt{p} (\sqrt{-1})^{\left(\frac{p-1}{2}\right)^2}.$$

Si l'on suppose que q est aussi un nombre premier impair, on aura par une simple permutation :

$$\sum_{t=0}^{t=q-1} e^{t \cdot \frac{2p\pi}{q}} \sqrt{-1} = \varepsilon \sqrt{q} (\sqrt{-1})^{\left(\frac{q-1}{2}\right)^2},$$

où $\varepsilon = +1$ ou $= -1$, selon que p est ou n'est pas résidu quadratique de q .

En multipliant les équations précédentes entre elles, il viendra :

$$\sum_{t=0}^{t=q-1} \sum_{s=0}^{s=p-1} e^{(qs+pt)\frac{2\pi}{pq}} V^{-1} = \delta \varepsilon \sqrt{pq} (\sqrt{-1})^{\binom{p-1}{2} + \binom{q-1}{2}},$$

ou ce qui est la même chose, en ajoutant $4st\pi\sqrt{-1}$ à l'exposant :

$$\sum_{t=0}^{t=q-1} \sum_{s=0}^{s=p-1} e^{(qs+pt)\frac{2\pi}{pq}} V^{-1} = \delta \varepsilon \sqrt{pq} (\sqrt{-1})^{\binom{p-1}{2} + \binom{q-1}{2}}.$$

Il est facile de voir qu'entre les limites de la double sommation $qs+pt$ ne saurait donner deux fois le même reste par rapport au diviseur pq ; car si les restes provenant de $qs+pt$ et de $qs'+pt'$ étaient égaux, $q(s-s')+p(t-t')$ serait divisible par pq , ce qui exige, s, s' étant compris entre 0 et $p-1$, et t, t' entre 0 et $q-1$, qu'on ait à la fois $s=s', t=t'$. Ces restes seront donc 0, 1, 2, ..., $pq-1$, et l'on pourra les mettre à la place de la série de valeurs fournies par l'expression $qs+pt$, ce changement consistant évidemment à négliger des multiples de $2\pi\sqrt{-1}$ dans l'exposant. On aura ainsi :

$$\sum_{s=0}^{s=pq-1} e^{s^2 \frac{2\pi}{pq}} V^{-1} = \delta \varepsilon \sqrt{pq} (\sqrt{-1})^{\binom{p-1}{2} + \binom{q-1}{2}}.$$

ou en remplaçant le premier membre par sa valeur qui résulte des expressions du paragraphe précédent :

$$\sqrt{pq} (\sqrt{-1})^{\binom{pq-1}{2}} = \delta \varepsilon \sqrt{pq} (\sqrt{-1})^{\binom{p-1}{2} + \binom{q-1}{2}},$$

et par conséquent :

$$\delta \varepsilon = (\sqrt{-1})^{\binom{pq-1}{2} - \binom{p-1}{2} - \binom{q-1}{2}},$$

et comme l'exposant est équivalent à l'expression :

$$\frac{1}{2}(p-1)(q-1) + (p-1)(q-1) \left(\frac{(p+1)(q+1)}{4} - 1 \right),$$

dont le second terme peut être négligé comme étant divisible par 4, il viendra :

$$\delta \varepsilon = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Cette équation renferme la loi de réciprocité, car il en résulte qu'on a $\delta = \varepsilon$, lorsque p et q sont l'un et l'autre de la forme $4\mu+1$, ou l'un de la forme $4\mu+1$, l'autre de la forme $4\mu+3$, et qu'au contraire on a $\delta = -\varepsilon$, lorsque p et q ont l'un et l'autre la forme $4\mu+3$.

SUR LES INTÉGRALES EULÉRIENNES.

PAR

M. G. LEJEUNE DIRICHLET.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 15 p. 258—263.

SUR LES INTÉGRALES EULÉRIENNES.

Les intégrales que LEGENDRE a appelées Eulériennes de première et de seconde espèce, sont celles que renferment les équations:

$$(1) \quad \int_0^1 (1-x)^{a-1} x^{b-1} dx = \int_0^x \frac{y^{a-1} dy}{(1+y)^{a+b}} = \left(\frac{b}{a}\right),$$

$$(2) \quad \int_0^1 \left(\log \frac{1}{x}\right)^{a-1} dx = \int_0^\infty e^{-y} y^{a-1} dy = \Gamma(a).$$

dans lesquelles les constantes a et b , ou du moins leurs parties réelles doivent être supposées positives pour que les intégrales ne deviennent pas infinies. EULER a fait voir qu'il y a entre ces deux transcendentes la relation très simple:

$$(3) \quad \left(\frac{b}{a}\right) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}.$$

Cette équation qui fait dépendre une intégrale de première espèce de trois intégrales de seconde espèce, renferme aussi une des principales propriétés de la fonction $\Gamma(a)$. En effet, si l'on y suppose $a+b=1$, on trouve, en ayant égard à l'équation évidente $\Gamma(1)=1$:

$$\Gamma(a)\Gamma(1-a) = \int_0^x \frac{y^{a-1} dy}{1+y}.$$

Or cette dernière intégrale a la valeur très simple $\frac{\pi}{\sin a\pi}$, comme EULER l'a trouvé par l'intégration d'une fraction rationnelle et comme on l'a vérifié de différentes manières. On a donc définitivement:

$$(4) \quad \Gamma(a)\Gamma(1-a) = \frac{\pi}{\sin a\pi}.$$

Pour établir l'équation (3) et les autres propriétés des intégrales Eulériennes, les géomètres ont employé des procédés assez différents. M. GAUSS part de l'équation:

$$(5) \quad \Gamma(a) = \frac{1.2.3\dots k}{a(a+1)(a+2)\dots(a+k-1)} k^{a-1}. \quad (k = \infty).$$

qui s'accorde avec la formule que LAPLACE a donnée pour exprimer la valeur approchée du produit $a(a+1)\dots(a+k-1)$, lorsqu'on y suppose k très grand. Après avoir démontré que l'expression (5) converge vers une limite déterminée lorsqu'on y fait croître indéfiniment l'entier positif k , M. GAUSS pose cette limite comme définition de $\Gamma(a)$ et déduit de là au moyen des séries et des produits infinis tous les théorèmes relatifs aux transcendentes Eulériennes, y compris les équations (1), (2) et (3). Cette marche très naturelle, lorsqu'on prend ce point de départ, ne l'est plus lorsqu'on définit ces transcendentes au moyen des équations (1) et (2), c'est-à-dire comme des intégrales. Il paraît alors plus simple et plus conforme à la définition de ces transcendentes de tout tirer du calcul intégral. L'équation (3) qui comprend la formule (4), ayant déjà été démontrée par MM. POISSON et JACOBI*), en transformant les intégrales qui y entrent, il reste pour rendre la théorie des intégrales Eulériennes plus uniforme, à prouver par l'intégration les autres formules qui s'y rapportent et particulièrement l'équation remarquable:

$$(6) \quad \Gamma(a)\Gamma\left(a+\frac{1}{n}\right)\Gamma\left(a+\frac{2}{n}\right)\dots\Gamma\left(a+\frac{n-1}{n}\right) = (2\pi)^{\frac{n-1}{2}} n^{1-na} \Gamma(na),$$

qui a été donnée par MM. GAUSS et LEGENDRE, mais qu'on n'a pas encore démontrée que je sache sans recourir aux développements infinis**). C'est l'objet que je vais remplir en peu de mots.

L'équation (2) donne par un simple changement de variable:

$$(7) \quad \int_0^{\infty} e^{-sy} y^{a-1} dy = \frac{\Gamma(a)}{s^a},$$

où s est une constante positive.

Si l'on y suppose $a = 1$, et que l'on intègre par rapport à s entre les limites 1 et s , on aura la formule connue:

$$(8) \quad \int_0^{\infty} (e^{-y} - e^{-sy}) \frac{dy}{y} = \log(s).$$

Si l'on différencie maintenant l'équation (2) par rapport à a , après y avoir remplacé y par s , on aura:

$$(9) \quad \int_0^{\infty} e^{-s} s^{a-1} \log(s) ds = \Gamma'(a),$$

*) Journal de l'École Polyt. 19^{ème} cahier p. 477. Journal de M. CRELLE, tome XI. p. 307.

**) Voyez sur ce point: Comment. Gottg. rec. vol. II., le Traité des fonctions elliptiques vol. II., les Exercices de M. CALCHOU 19^{ème} livraison et un Mémoire de M. CRELLE tome VII. p. 375 de son Journal.

où l'on a fait pour abrégér:

$$\frac{d\Gamma(a)}{da} = \Gamma'(a).$$

Substituant pour $\log(s)$ l'intégrale (8), et intervertissant l'ordre des intégrations, il vient:

$$\int_0^x \frac{dy}{y} \left(e^{-y} \int_0^x e^{-s} s^{a-1} ds - \int_0^x e^{-(1+y)s} s^{a-1} ds \right) = \Gamma'(a),$$

ou, si l'on met en vertu des équations (2) et (7), $\Gamma'(a)$, $\frac{\Gamma'(a)}{(1+y)^a}$ à la place des deux intégrales relatives à s :

$$(10) \quad \Gamma(a) \int_0^x \frac{dy}{y} \left(e^{-y} - \frac{1}{(1+y)^a} \right) = \Gamma'(a),$$

équation qu'on peut mettre sous cette autre forme, en introduisant une nouvelle variable x telle que $x = \frac{1}{1+y}$:

$$(11) \quad \int_0^1 \left(e^{1-\frac{1}{x}} - x^a \right) \frac{dx}{x(1-x)} = \frac{\Gamma'(a)}{\Gamma(a)} = \frac{d \log \Gamma(a)}{da}.$$

Mettant $a, a + \frac{1}{n}, a + \frac{2}{n}, \dots, a + \frac{n-1}{n}$, où n désigne un entier positif indépendant de a , à la place de a et faisant la somme de toutes ces équations, on aura:

$$\int_0^1 \left[n e^{1-\frac{1}{x}} - x^a \left(1 + x^{\frac{1}{n}} + x^{\frac{2}{n}} + \dots + x^{\frac{n-1}{n}} \right) \right] \frac{dx}{x(1-x)} = S,$$

si l'on fait pour abrégér:

$$S = \frac{d \log \Gamma(a)}{da} + \frac{d \log \Gamma\left(a + \frac{1}{n}\right)}{da} + \dots + \frac{d \log \Gamma\left(a + \frac{n-1}{n}\right)}{da},$$

ou ce qui revient au même:

$$\int_0^1 \left(\frac{n e^{1-\frac{1}{x}}}{1-x} - \frac{x^a}{1-x^{\frac{1}{n}}} \right) \frac{dx}{x} = S.$$

Remplaçant x par x^n , cette équation deviendra:

$$n \int_0^1 \left(\frac{n e^{1-\frac{1}{x^n}}}{1-x^n} - \frac{x^{na}}{1-x} \right) \frac{dx}{x} = S.$$

Si l'on retranche de cette équation l'équation (11), après avoir multiplié celle-ci par n et y avoir remplacé a par na , on trouve, en remettant pour S sa valeur

et en remarquant qu'on a $n \frac{\Gamma'(na)}{\Gamma(na)} = \frac{d \log \Gamma(na)}{da}$:

$$\int_0^1 \left(\frac{n^e \frac{1-x}{x^n}}{1-x^n} - \frac{e^{\frac{1-x}{x}}}{1-x} \right) \frac{dx}{x} = \frac{d}{da} \log \left(\frac{\Gamma(a)\Gamma\left(a+\frac{1}{n}\right)\dots\Gamma\left(a+\frac{n-1}{n}\right)}{\Gamma(na)} \right).$$

Désignant par $\log(p)$ le premier membre de cette équation, qui ne dépend pas de a , intégrant par rapport à a et passant des logarithmes aux nombres, on aura:

$$(12) \quad \Gamma(a)\Gamma\left(a+\frac{1}{n}\right)\dots\Gamma\left(a+\frac{n-1}{n}\right) = qp^n \Gamma(na),$$

où q est la constante introduite par l'intégration. Pour déterminer les quantités p et q , l'une et l'autre indépendantes de a , on changera a en $a+\frac{1}{n}$. Dis-
visant l'équation qui résulte de ce changement par l'équation (12), on trouve:

$$\frac{\Gamma(a+1)}{\Gamma(a)} = p^{\frac{1}{n}} \frac{\Gamma(na+1)}{\Gamma(na)},$$

d'où l'on conclut en vertu de l'équation connue $\Gamma(b+1) = b\Gamma(b)$:

$$p = n^n.$$

L'équation (12) devient ainsi:

$$\Gamma(a)\Gamma\left(a+\frac{1}{n}\right)\dots\Gamma\left(a+\frac{n-1}{n}\right) = qn^{-na}\Gamma(na).$$

Pour déterminer q , on fera $a = \frac{1}{n}$, ce qui donne:

$$\Gamma\left(\frac{1}{n}\right)\Gamma\left(\frac{2}{n}\right)\dots\Gamma\left(\frac{n-1}{n}\right) = \frac{1}{n} q.$$

Si l'on écrit cette équation une seconde fois en renversant l'ordre des facteurs et si l'on forme ensuite le produit des deux équations, en évaluant le produit de deux facteurs de même rang au moyen de la formule (4), on obtient:

$$\frac{\pi}{\sin \frac{\pi}{n}} \cdot \frac{\pi}{\sin \frac{2\pi}{n}} \cdots \frac{\pi}{\sin \frac{(n-1)\pi}{n}} = \frac{1}{n^2} q^2;$$

substituant pour le premier membre sa valeur connue, on conclut:

$$q = (2\pi)^{\frac{n-1}{2}} \sqrt{n}.$$

On a donc définitivement:

$$\Gamma(a)\Gamma\left(a+\frac{1}{n}\right)\Gamma\left(a+\frac{2}{n}\right)\dots\Gamma\left(a+\frac{n-1}{n}\right) = (2\pi)^{\frac{n-1}{2}} n^{1-na} \Gamma(na),$$

ce qui coïncide avec l'équation (6).

L'équation (11) diffère un peu par sa forme de l'équation connue:

$$(13) \quad \int_0^1 \left(\frac{1}{\log\left(\frac{1}{x}\right)} - \frac{x^{n-1}}{1-x} \right) dx = \frac{d \log \Gamma(a)}{da}.$$

Pour obtenir cette dernière, il faut transformer d'une manière différente les deux parties de l'intégrale (10). En posant, comme plus haut, $x = \frac{1}{1+y}$ dans la seconde, il faut, dans la première qui contient l'exponentielle e^{-y} , remplacer y par $\log\left(\frac{1}{x}\right)$. Mais ce procédé n'est pas exempt de difficulté, car on sait qu'il n'est pas permis en général d'employer des substitutions différentes dans deux parties d'une intégrale, lorsque ces parties sont séparément infinies. Pour se convaincre que dans le cas actuel le résultat auquel on arrive en opérant comme on vient de le dire, est néanmoins exact, on remarquera que, puisque la fonction sous le signe d'intégration dans l'intégrale (10) ne devient pas infinie pour $y = 0$, la différence entre cette intégrale et l'expression:

$$(14) \quad \int_{\varepsilon}^{\infty} \left(e^{-y} - \frac{1}{(1+y)^{\varepsilon}} \right) \frac{dy}{y}$$

deviendra moindre que toute quantité assignable, lorsqu'on fait décroître indéfiniment le nombre positif ε . En effectuant dans l'intégrale (14) les deux substitutions indiquées, elle prendra cette forme:

$$\int_0^{e^{-\varepsilon}} \frac{dx}{\log\left(\frac{1}{x}\right)} - \int_0^{\frac{1}{1+\varepsilon}} \frac{x^{\varepsilon-1} dx}{1-x},$$

ou, ce qui est la même chose, en ajoutant et en retranchant en même temps

$$\text{l'intégrale } \int_{e^{-\varepsilon}}^{\frac{1}{1+\varepsilon}} \frac{dx}{\log\left(\frac{1}{x}\right)} :$$

$$(15) \quad \int_0^{\frac{1}{1+\varepsilon}} \left(\frac{1}{\log\left(\frac{1}{x}\right)} - \frac{x^{\varepsilon-1}}{1-x} \right) dx - \int_{e^{-\varepsilon}}^{\frac{1}{1+\varepsilon}} \frac{dx}{\log\left(\frac{1}{x}\right)}.$$

La fonction sous le signe d'intégration dans la dernière de ces deux intégrales qui est du genre de celles que M. CAUCHY appelle singulières, croissant lorsque x passe de la limite inférieure à la limite supérieure, cette intégrale est évidemment moindre que la quantité:

$$\left(\frac{1}{1+\varepsilon} - e^{-\varepsilon} \right) \frac{1}{\log(1+\varepsilon)},$$

qui devient infiniment petite en même temps que ε . Il suit de là et de ce qui précède, que la première des intégrales (15) finira par différer de l'intégrale (10) d'une quantité moindre que toute grandeur assignable. D'un autre côté, comme

la fonction $\frac{1}{\log\left(\frac{1}{x}\right)} - \frac{x^{a-1}}{1-x}$ a une valeur finie pour $x = 1$, cette même intégrale (15) converge aussi pour des valeurs décroissantes de ε vers la limite:

$$\int_0^1 \left(\frac{1}{\log\left(\frac{1}{x}\right)} - \frac{x^{a-1}}{1-x} \right) dx.$$

qui doit par conséquent coïncider avec l'intégrale (10); ce qui montre l'accord des équations (10) et (13).

Je ferai remarquer encore que l'équation (3), après y avoir remplacé $\left(\frac{b}{a}\right)$ par l'intégrale (1), étant différenciée logarithmiquement par rapport à b , donne d'abord:

$$\int_0^1 (1-x)^{a-1} x^{b-1} \log(x) dx = \left(\frac{\Gamma'(b)}{\Gamma(b)} - \frac{\Gamma'(a+b)}{\Gamma(a+b)} \right) \int_0^1 (1-x)^{a-1} x^{b-1} dx,$$

et par suite, en ayant égard à l'équation (11):

$$\int_0^1 (1-x)^{a-1} x^{b-1} \log\left(\frac{1}{x}\right) dx = \int_0^1 x^{b-1} \frac{(1-x^a)}{1-x} dx \cdot \int_0^1 (1-x)^{a-1} x^{b-1} dx,$$

théorème connu qu'EULER a déduit de la considération d'un produit composé d'un nombre infini de facteurs.

En terminant je démontrerai une équation qui comprend la formule (3). L'équation (7) donne, en y mettant $c+z$ à la place de s :

$$\int_0^\infty e^{-(c+z)y} y^{a-1} dy = \frac{\Gamma(a)}{(c+z)^a}.$$

Multipliant celle-ci par $e^{kz} z^{b-1} dz$, b et k désignant ainsi que a et c des constantes positives, et intégrant depuis $z = 0$ jusqu'à $z = \infty$, il vient:

$$\int_0^\infty e^{-cy} y^{a-1} dy \int_0^\infty e^{-(k+y)z} z^{b-1} dz = \Gamma(a) \int_0^\infty \frac{e^{-kz} z^{b-1}}{(c+z)^a} dz,$$

équation qui prend cette autre forme, si l'on y met pour l'intégrale relative à z dans le premier membre sa valeur donnée par la formule (7):

$$\Gamma(b) \int_0^\infty \frac{e^{-cy} y^{a-1}}{(k+y)^b} dy = \Gamma(a) \int_0^\infty \frac{e^{-kz} z^{b-1}}{(c+z)^a} dz.$$

Cette relation entre deux transcendentes de même forme rentre dans l'équation (3) lorsqu'on fait $c = 0$, $k = 1$. Il faut dans ce cas, pour que les deux membres ne deviennent pas infinis, supposer $b > a$; mettant donc $a+b$ à la place de b , on aura précisément l'équation (3).

UEBER
DIE METHODE DER KLEINSTEN QUADRATE.

VON

G. LÉJEUNE DIRICHLET.

UEBER DIE METHODE DER KLEINSTEN QUADRATE.

[Auszug aus einer in der Akademie der Wissenschaften am 28. Juli 1836 gelesenen Abhandlung „über die Frage, in wiefern die Methode der kleinsten Quadrate bei sehr zahlreichen Beobachtungen unter allen linearen Verbindungen der Bedingungsgleichungen als das vortheilhafteste Mittel zur Bestimmung unbekannter Elemente zu betrachten sei“.]

Der von LAPLACE in seiner „Théorie analytique des probabilités“ gegebene Beweis beruht wesentlich auf der Voraussetzung, dass die verschiedenen Factorsysteme, zwischen denen man zu wählen hat, von den in den Gleichungen enthaltenen constanten Gliedern nicht abhängen. Hebt man diese Beschränkung auf, so lassen sich Factorsysteme angeben, die von demjenigen, welches der Methode der kleinsten Quadrate entspricht, ganz verschieden sind, und im Allgemeinen eine ebenso grosse Genauigkeit zu erwarten erlauben. Das einfachste Beispiel dieser Art liefert das bekannte Verfahren, den Werth einer Constante, welche unmittelbarer Gegenstand der Beobachtung ist, dadurch zu bestimmen, dass man die von einer grossen ungeraden Anzahl von Beobachtungen gegebenen Werthe ihrer Grösse nach ordnet, und den in der Mitte liegenden für die Unbekannte wählt. Sucht man die Grenzen, innerhalb welcher der Fehler des so bestimmten Werthes mit einer gegebenen Wahrscheinlichkeit liegt, und vergleicht diese Grenzen mit denen, welche dem arithmetischen Mittel entsprechen, in welches für den vorliegenden Fall das Resultat der Methode der kleinsten Quadrate übergeht, so ergibt sich, dass bei gleicher Wahrscheinlichkeit die Fehlergrenzen für beide Methoden sich wie die Constanten:

$$\frac{1}{\sqrt{2}f(0)} \quad \text{und} \quad 2 \int_0^a x^2 f(x) dx$$

zu einander verhalten. Die Function $f(x)$, welche der Bedingung $f(-x) = f(x)$ unterworfen ist, drückt das Gesetz der Beobachtungsfehler aus, welche immer zwischen $-a$ und $+a$ liegend angenommen werden. Es ist klar, dass sich im Allgemeinen, d. h. so lange man keine Voraussetzung über die Function $f(x)$ macht, nicht entscheiden lässt, welche jener Constanten grösser ist, und es bleibt mithin ungewiss, ob das arithmetische Mittel oder das andere Verfahren den Vorzug verdient.

SUR LES SÉRIES DONT LE TERME GÉNÉRAL
DÉPEND DE DEUX ANGLES, ET QUI SERVENT
A EXPRIMER DES FONCTIONS ARBITRAIRES
ENTRE DES LIMITES DONNÉES.

PAR

G. LEJEUNE DIRICHLET,
PROF. A L'UNIVERSITÉ DE BERLIN.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 17 p. 35—56.

SUR LES SÉRIES
DONT LE TERME GÉNÉRAL DÉPEND DE DEUX ANGLES,
ET QUI SERVENT A EXPRIMER DES FONCTIONS ARBITRAIRES
ENTRE DES LIMITES DONNÉES.

Les séries que nous nous proposons de considérer, dans ce Mémoire, sont ordonnées suivant des fonctions d'une forme particulière, fonctions dont LEGENDRE a le premier fait usage dans ses belles recherches sur l'attraction des ellipsoïdes de révolution et sur la figure des planètes. Ces fonctions jouissent d'un grand nombre de propriétés remarquables et les séries qui en sont formées, sont propres à représenter des fonctions arbitraires entre certaines limites. La généralité de cette dernière proposition n'ayant pas été jugée suffisamment établie*) par les considérations qui amènent les développements de ce genre dans la théorie de l'attraction des sphéroïdes, on a cherché à la prouver d'une manière directe et indépendante de cette théorie.

Si l'on désigne par P_n le coefficient de a^n dans la valeur développée du radical:

$$\frac{1}{\sqrt{1-2a(\cos\theta\cos\theta'+\sin\theta\sin\theta'\cos(q'-q))+a^2}}$$

la proposition dont il s'agit, sera exprimée par l'équation:

$$(a) \quad f(\theta, q) = \frac{1}{4\pi} \sum_{n=0}^{n=\infty} (2n+1) \int_0^\pi d\theta' \sin\theta' \int_0^{2\pi} P_n f(\theta', q') dq',$$

qui a lieu pour toutes les valeurs de θ et de q comprises entre les limites $\theta = 0$ et $\theta = \pi$, $q = 0$ et $q = 2\pi$, la fonction $f(\theta, q)$ restant entièrement arbitraire entre ces limites et étant seulement assujettie à ne pas devenir infinie. En ayant égard à l'origine de P_n , on prouve que ce coefficient considéré comme fonction des deux angles θ et q , est une expression rationnelle et entière du degré n des trois quantités $\cos\theta$, $\sin\theta\cos q$, $\sin\theta\sin q$, qui satisfait à

*) Mécanique céleste, tome II. p. 72.

cette équation aux différences partielles:

$$(b) \quad \frac{1}{\sin \theta} \cdot \frac{\partial \left(\sin \theta \frac{\partial P_n}{\partial \theta} \right)}{\partial \theta} + \frac{1}{\sin^2 \theta} \cdot \frac{\partial^2 P_n}{\partial \varphi^2} + n(n+1)P_n = 0.$$

Comme les intégrations, dans l'équation (a), ont lieu entre des limites constantes et sont relatives à des variables indépendantes de θ et de φ , il est évident que le terme général:

$$X_n = \frac{2n+1}{4\pi} \int_0^\pi d\theta' \sin \theta' \int_0^{2\pi} P_n f(\theta', \varphi') d\varphi'$$

sera aussi une fonction rationnelle et entière du degré n de $\cos \theta$, $\sin \theta \cos \varphi$, $\sin \theta \sin \varphi$, et qui satisfera pareillement à l'équation:

$$(c) \quad \frac{1}{\sin \theta} \cdot \frac{\partial \left(\sin \theta \frac{\partial X_n}{\partial \theta} \right)}{\partial \theta} + \frac{1}{\sin^2 \theta} \cdot \frac{\partial^2 X_n}{\partial \varphi^2} + n(n+1)X_n = 0.$$

La proposition citée revient donc à dire qu'une fonction quelconque $f(\theta, \varphi)$ de deux variables peut être exprimée, pour toutes les valeurs de θ et φ comprises entre les limites indiquées, par une série de la forme:

$$f(\theta, \varphi) = X_0 + X_1 + X_2 + \dots + X_n + \dots,$$

dans laquelle X_n est une fonction rationnelle et entière du degré n de $\cos \theta$, $\sin \theta \cos \varphi$, $\sin \theta \sin \varphi$, telle que l'équation (c) ait lieu. M. POISSON qui a appliqué la série (a) à des questions très variées de physique et de mécanique, en a donné une démonstration qui revient à peu près à ce qui suit*). Il suppose que les termes de cette série sont multipliés par les puissances successives d'une fraction positive α , c'est-à-dire qu'il considère la série:

$$\frac{1}{4\pi} \iint f(\theta', \varphi') \sin \theta' d\theta' d\varphi' \sum (2n+1) P_n \alpha^n.$$

L'opération indiquée par le signe \sum étant effectuée, il fait voir que l'intégrale double qui exprime la somme de la série ainsi modifiée, converge vers la limite $f(\theta, \varphi)$, lorsque la fraction α converge vers l'unité. De ce résultat que LAGRANGE avait déjà obtenu d'une autre manière**), il conclut l'équation (a) en posant $\alpha = 1$. On voit que cette manière de procéder renferme implicite-

*) Journal de l'École Polyt., 19^{me} cah. p. 145: Additions à la connaissance des temps pour l'an 1829 et pour l'an 1831. Théorie math. de la chaleur, p. 212.

**) Journal de l'École Polyt., 15^{me} cah. p. 66.

ment deux suppositions. On admet que la série précédente dont la convergence est évidente tant que la quantité a reste inférieure à l'unité, conserve encore cette propriété pour $a = 1$. On suppose encore que la valeur de la série correspondante à $a = 1$, est en effet la limite de celle qui a lieu pour une fraction qu'on suppose converger vers l'unité. Cette seconde supposition ne doit pas paraître évidente: car il existe des séries dont les termes sont des fonctions continues d'une même variable a , et qui changent néanmoins d'une quantité finie lorsque la variable varie infiniment peu. Mais cette circonstance ne saurait avoir lieu dans le cas actuel, car l'on peut prouver généralement que les séries ordonnées suivant les puissances d'une variable a , sont nécessairement des fonctions continues de cette variable, tant qu'elles restent convergentes*). Tout se réduit donc à prouver que la série (a) est convergente.

Pour établir ce point essentiel, l'illustre auteur transforme le terme général au moyen de l'intégration par parties deux fois appliquée à chacune des variables θ' , q' et en ayant égard à l'équation (b). Les termes que cette double opération fait sortir du signe, se détruisant aux limites, il introduit dans l'intégrale transformée l'expression approchée que LAPLACE a donnée pour P_n lorsque l'indice n est très grand, et il conclut que les termes très éloignés de la série (a) finissent par devenir inférieurs à $\frac{A}{n\sqrt{n}}$, A désignant une constante**). Ce résultat étant supposé avoir lieu, la convergence de la série s'ensuit rigoureusement. Mais pour y parvenir, M. POISSON est obligé de faire plusieurs suppositions qui peuvent n'avoir pas lieu. Il suppose que les coefficients différentiels du premier et du second ordre de $f(\theta', q')$ relatifs à l'une et à l'autre des variables restent finis, il suppose de plus que la fonction $f(\theta', q')$ devient indépendante de q' , lorsqu'on y pose $\theta' = 0$. Outre ces restrictions que M. POISSON énonce, il y en a d'autres qui sont également nécessaires pour le succès de son analyse. Il faut encore, que $f(\theta', q')$ et ses deux dérivées $\frac{\partial f(\theta', q')}{\partial \theta'}$, $\frac{\partial f(\theta', q')}{\partial q'}$ soient des fonctions continues, car si cette circonstance n'avait pas lieu, les termes que l'intégration par parties fait sortir du signe, subsisteraient quoiqu'ils disparaissent aux limites des intégrations.

*) Voyez sur ce point un Mémoire de l'illustre ABEL. Tome I. p. 314 du Journal de CRELLE.)

**) Connaissance des temps pour 1831.

¹⁾ Oeuvres complètes de NIELS HENRIK ABEL, 1851. Tome I. p. 223. K.

Les différentes circonstances dont la transformation qu'on vient d'indiquer exige l'absence, peuvent se trouver réunies dans des cas très simples. Supposons par exemple, que la fonction $f(\theta', \varphi')$ ne renferme que θ' , et soit exprimée par $\cos^k \theta'$ (k désignant une constante positive inférieure à l'unité) tant que $\theta' < \frac{1}{2}\pi$, et égale à zéro lorsque $\theta' > \frac{1}{2}\pi$. Dans cet exemple auquel M. POISSON a appliqué la série $(a)^*$, la fonction $f(\theta')$ est continue, mais il n'en est pas de même de son coefficient différentiel, qui devient infini pour $\theta' = \frac{1}{2}\pi$ et passe ensuite brusquement à la valeur zéro, qu'il conserve dans tout l'intervalle compris entre $\theta' = \frac{1}{2}\pi$ et $\theta' = \pi$. Dans ce cas particulier, le terme général transformé se présente comme la différence de deux quantités infinies.

Il y a, au reste, une remarque générale à faire sur la série (a) , qui s'applique également à toutes les autres formes de développement propres à représenter des fonctions arbitraires, c'est-à-dire des fonctions qui ne sont assujetties à aucune loi analytique. Les séries de ce genre, quoique toujours convergentes lorsque la fonction qu'elles développent, ne devient pas infinie, ne jouissent pas toujours de cette propriété en vertu du seul décroissement de leurs termes. Il existe des cas pour lesquels cette convergence résulte de la manière dont les termes consécutifs se détruisent en partie par l'opposition des signes, en sorte que les termes réduits à leurs valeurs numériques, formeraient une série divergente, et si une démonstration complète de la convergence de ces sortes de développements présente quelque difficulté, elle tient surtout à la possibilité de pareils cas. Quoi qu'il en soit, il résulte du moins de cette remarque très simple et qu'il serait facile de justifier par de nombreux exemples que tout moyen de démonstration qui n'aurait égard qu'au seul décroissement des termes, est nécessairement incomplet et ne saurait embrasser tous les cas.

Il existe un autre procédé qu'on peut appliquer aux questions de ce genre, procédé exempt des difficultés qu'on vient d'indiquer, et qui dérive d'ailleurs naturellement de l'idée que l'on doit se faire de la somme d'une suite infinie. Une pareille somme n'étant autre chose que la limite vers laquelle converge la somme des n premiers termes, lorsque n devient de plus en plus grand, on parviendra à une démonstration complète en déterminant la limite dont il s'agit. C'est ce procédé que j'ai déjà employé pour démontrer la for-

^{*)} Connaissance des temps pour 1829 p. 348.

mule qui exprime une fonction arbitraire par une série ordonnée suivant les sinus et les cosinus des multiples de la variable*).

L'application du même moyen de démonstration à la série (α) est moins facile, non seulement parce que les termes de cette série sont donnés par une double intégration, mais surtout parce que, la fonction P_n étant plus compliquée qu'un simple sinus ou cosinus, il faut introduire une nouvelle expression intégrale pour pouvoir exécuter l'intégration aux différences finies étendue à un nombre indéterminé de termes. Néanmoins, si l'on met P_n d'une manière convenable sous forme d'intégrale définie, la somme des n premiers termes de la série prend une forme assez simple et la limite vers laquelle converge cette somme, pour des valeurs croissantes de n , résulte du même théorème dont j'ai déjà fait usage dans le Mémoire cité. Je commence par quelques recherches préliminaires sur le coefficient P_n .

§. 1.

Si l'on désigne par γ un angle réel que nous supposons compris entre 0 et π , et par α une fraction positive ou négative, le radical $\frac{1}{\sqrt{1-2\alpha\cos\gamma+\alpha^2}}$ peut être développé suivant les puissances positives de α :

$$(1) \quad \frac{1}{\sqrt{1-2\alpha\cos\gamma+\alpha^2}} = P_0 + P_1\alpha + P_2\alpha^2 + \dots + P_n\alpha^n + \dots$$

Le coefficient P_n est, comme l'on sait, une fonction rationnelle et entière de $\cos\gamma$, ayant pour expression:

$$(2) \quad P_n = \frac{1.3.5\dots(2n-1)}{1.2.3\dots n} \left[\cos^n\gamma - \frac{n(n-1)}{2(2n-2)} \cos^{n-2}\gamma + \frac{n(n-1)(n-2)(n-3)}{2.4(2n-1)(2n-3)} \cos^{n-4}\gamma - \dots \right].$$

Je ferai observer, en passant, qu'on a aussi:

$$P_n = 1 - \frac{(n+1)n}{1^2} \sin^2 \frac{\gamma}{2} + \frac{(n+2)(n+1)n(n-1)}{1^2.2^2} \sin^4 \frac{\gamma}{2} - \frac{(n+3)(n+2)\dots(n-2)}{1^2.2^2.3^2} \sin^6 \frac{\gamma}{2} + \dots$$

$$P_n = (-1)^n \left[1 - \frac{(n+1)n}{1^2} \cos^2 \frac{\gamma}{2} + \frac{(n+2)(n+1)n(n-1)}{1^2.2^2} \cos^4 \frac{\gamma}{2} - \frac{(n+3)(n+2)\dots(n-2)}{1^2.2^2.3^2} \cos^6 \frac{\gamma}{2} + \dots \right],$$

*) Journal de CRELLE, Vol. IV, p. 157.)

*) S. 117 dieser Ausgabe von G. Lejeune Dirichlet's Werke. K.

$$P_n = \cos^n \frac{\gamma}{2} \left[1 - \binom{n}{1} \tan^2 \frac{\gamma}{2} + \binom{n(n-1)}{1.2} \tan^4 \frac{\gamma}{2} - \binom{n(n-1)(n-2)}{1.2.3} \tan^6 \frac{\gamma}{2} + \dots \right].$$

Ces expressions très simples et qui sont faciles à démontrer, ne paraissent pas avoir été remarquées.

Le même coefficient peut être développé suivant les cosinus des multiples de γ *) :

$$\begin{aligned} \frac{1}{2} P_n &= \frac{1.3 \dots (2n-1)}{2.4 \dots 2n} \cos n\gamma + \frac{1.3 \dots (2n-3)}{2.4 \dots (2n-2)} \cdot \frac{1}{2} \cos(n-2)\gamma \\ &+ \frac{1.3 \dots (2n-5)}{2.4 \dots (2n-4)} \cdot \frac{1.3}{2.4} \cos(n-4)\gamma + \dots \end{aligned}$$

expression qui a l'avantage de faire voir que la valeur numérique de P_n ne surpasse jamais l'unité. En effet, les coefficients de $\cos n\gamma$, $\cos(n-2)\gamma$, ... étant tous positifs, il est évident que la valeur numérique de P_n correspondant à une valeur quelconque de γ ne saurait surpasser celle qui a lieu pour $\gamma = 0$, et il résulte d'un autre côté de l'équation (1), que, dans ce cas particulier, P_n se réduit à l'unité.

LAPLACE a fait voir que P_n peut être exprimé par cette intégrale définie**):

$$P_n = \frac{1}{\pi} \int_0^\pi [\cos \gamma - \sin \gamma \cos \psi]^{-1} d\psi.$$

C'est de cette expression de P_n que l'illustre géomètre a conclu la valeur approchée dont il a été question plus haut***). Il y est parvenu au moyen de la belle méthode dont l'Analyse lui est redevable et qui a pour objet d'obtenir les valeurs finales des intégrales définies où il entre sous le signe d'intégration des exposants qu'on suppose de plus en plus grands.

L'objet de ce Mémoire exige que nous mettions P_n sous forme d'intégrale définie. L'expression précédente ne se prêtant pas bien aux calculs que nous avons à faire, à cause des quantités imaginaires qui y entrent et qu'on ne saurait chasser sans que l'entier n paraisse à la fois comme exposant et comme facteur sous le signe trigonométrique, nous allons chercher une autre intégrale plus appropriée à la recherche qui nous occupe. Pour obtenir cette

*) Exercices de calcul intégral, tome II, p. 248.

***) Mécanique céleste, tome V, p. 32.

****) Mécanique céleste, tome V, p. 33. Voyez aussi le supplément au tome V, p. 2.

nouvelle expression de P_n , remplaçons dans l'équation (1), α par $e^{i\psi V^{-1}}$, ψ désignant un angle indépendant de γ et compris comme ce dernier entre 0 et π .

Le second membre de cette équation prendra la forme $G + H\sqrt{-1}$, en posant pour abrégér:

$$G = P_0 + P_1 \cos \psi + P_2 \cos 2\psi + \dots + P_n \cos n\psi + \dots,$$

$$H = P_1 \sin \psi + P_2 \sin 2\psi + \dots + P_n \sin n\psi + \dots$$

Quant au premier membre, on trouve que sa partie réelle a une expression différente selon que ψ est inférieur ou supérieur à γ , et qu'il en est de même du coefficient de $\sqrt{-1}$. Cette partie réelle étant dans le premier cas,

$$\frac{\cos \frac{1}{2} \psi}{\sqrt{2(\cos \psi - \cos \gamma)}}, \text{ et dans le second, } \frac{\sin \frac{1}{2} \psi}{\sqrt{2(\cos \gamma - \cos \psi)}}, \text{ on aura aussi:}$$

$$G = \frac{\cos \frac{1}{2} \psi}{\sqrt{2(\cos \psi - \cos \gamma)}} \quad \text{ou} \quad G = \frac{\sin \frac{1}{2} \psi}{\sqrt{2(\cos \gamma - \cos \psi)}}.$$

selon que $\psi < \gamma$ ou $\psi > \gamma$. On trouve pareillement:

$$H = \frac{-\sin \frac{1}{2} \psi}{\sqrt{2(\cos \psi - \cos \gamma)}} \quad \text{ou} \quad H = \frac{\cos \frac{1}{2} \psi}{\sqrt{2(\cos \gamma - \cos \psi)}}.$$

selon que $\psi < \gamma$ ou $\psi > \gamma$.

On a d'un autre côté, par la théorie connue des séries de sinus et de cosinus:

$$P_n = \frac{2}{\pi} \int_0^\gamma G \cos n\psi d\psi \quad \text{et} \quad P_n = \frac{2}{\pi} \int_0^\gamma H \sin n\psi d\psi.$$

Si l'on partage chacune de ces intégrales en deux autres prises entre les limites 0 et γ , γ et π , et qu'on mette ensuite pour G et H leurs valeurs données plus haut, il viendra:

$$(3) \quad P_n = \frac{2}{\pi} \int_0^\gamma \frac{\cos n\psi \cos \frac{1}{2} \psi d\psi}{\sqrt{2(\cos \psi - \cos \gamma)}} + \frac{2}{\pi} \int_\gamma^\pi \frac{\cos n\psi \sin \frac{1}{2} \psi d\psi}{\sqrt{2(\cos \gamma - \cos \psi)}}.$$

$$(4) \quad P_n = -\frac{2}{\pi} \int_0^\gamma \frac{\sin n\psi \sin \frac{1}{2} \psi d\psi}{\sqrt{2(\cos \psi - \cos \gamma)}} + \frac{2}{\pi} \int_\gamma^\pi \frac{\sin n\psi \cos \frac{1}{2} \psi d\psi}{\sqrt{2(\cos \gamma - \cos \psi)}}.$$

où il est essentiel de remarquer que, d'après la théorie citée, le second membre de l'équation (3) doit être réduit à moitié lorsque $n = 0$, et que l'équation (4) ne s'applique pas à ce cas, P_0 n'entrant pas dans la série H .

Le procédé qui vient de nous conduire à cette double expression de P_n , n'est pas rigoureux en ce que nous n'avons pas démontré que les séries G et

Il sont convergentes. Cette convergence a effectivement lieu, le cas excepté où $\psi = \gamma$, pour lequel les fonctions de ψ que ces séries représentent, deviennent infinies. Mais comme la considération de ces séries exigerait trop de détails, nous ne nous y arrêtons pas et nous allons faire voir, à posteriori, et par un calcul très simple que les intégrales précédentes expriment en effet les coefficients du développement du radical:

$$\frac{1}{\sqrt{1-2a\cos\gamma+a^2}}.$$

Si l'on désigne par Q_n la première des deux intégrales contenues dans l'équation (3), on aura:

$$Q_n = \frac{2}{\pi} \int_0^\gamma \frac{\cos n\psi \cos \frac{1}{2}\psi}{\sqrt{2(\cos\psi - \cos\gamma)}} d\psi$$

et la valeur numérique de Q_n sera évidemment inférieure à:

$$\frac{2}{\pi} \int_0^\gamma \frac{\cos \frac{1}{2}\psi d\psi}{\sqrt{2(\cos\psi - \cos\gamma)}} = 1.$$

La série:

$$\frac{1}{2}Q_0 + Q_1a + Q_2a^2 + \dots + Q_n a^n + \dots$$

dans laquelle a désigne une fraction positive ou négative, sera donc convergente. Pour en obtenir la somme, mettons à la place de Q_0, Q_1, Q_2, \dots ce que ces lettres représentent. Il viendra ainsi:

$$\frac{2}{\pi} \int_0^\gamma \frac{\cos \frac{1}{2}\psi d\psi}{\sqrt{2(\cos\psi - \cos\gamma)}} (\frac{1}{2} + a\cos\psi + a^2\cos 2\psi + \dots)$$

ou, si l'on remplace dans l'intégrale la série convergente par sa valeur connue

$$\frac{1}{2} \frac{1-a^2}{1-2a\cos\psi+a^2} :$$

$$\frac{1-a^2}{\pi} \int_0^\gamma \frac{\cos \frac{1}{2}\psi d\psi}{\sqrt{2(\cos\psi - \cos\gamma)}} \cdot \frac{1}{1-2a\cos\psi+a^2}.$$

L'introduction d'une nouvelle variable s telle que $s \sin \frac{\gamma}{2} = \sin \frac{\psi}{2}$, changera l'intégrale en celle-ci:

$$\frac{1-a^2}{\pi} \int_0^1 \frac{ds}{\sqrt{1-s^2}} \cdot \frac{1}{(1-a)^2 + 4as^2 \sin^2 \frac{1}{2}\gamma}.$$

L'intégration étant effectuée par les méthodes connues, on trouve:

$$\frac{1}{2} \frac{1+a}{1-2a\cos\gamma+a^2} = \frac{1}{2}Q_0 + Q_1a + Q_2a^2 + \dots + Q_n a^n + \dots$$

On pourrait obtenir d'une manière semblable la somme de la série:

$$\frac{1}{2} R_0 + R_1 \alpha + R_2 \alpha^2 + \dots + R_n \alpha^n + \dots,$$

R_n désignant pour abrégé la seconde des intégrales (3). Mais on y parvient plus simplement par la considération suivante. Le terme général:

$$R_n \alpha^n = \frac{2}{\pi} \alpha^n \int_{\gamma}^{\pi} \frac{\cos n \psi \sin \frac{1}{2} \psi d\psi}{\sqrt{2(\cos \gamma - \cos \psi)}}$$

prendra cette autre forme, si l'on remplace ψ par $\pi - \psi$, et que l'on observe qu'on a $\cos n(\pi - \psi) = (-1)^n \cos n \psi$:

$$\frac{2}{\pi} (-\alpha)^n \int_0^{\pi-\gamma} \frac{\cos n \psi \cos \frac{1}{2} \psi d\psi}{\sqrt{2(\cos \psi - \cos(\pi - \gamma))}}.$$

Sous cette forme, il est évident que ce terme général résulte de celui de la série déjà sommée et qui est:

$$Q_n \alpha^n = \frac{2}{\pi} \alpha^n \int_0^{\gamma} \frac{\cos n \psi \cos \frac{1}{2} \psi d\psi}{\sqrt{2(\cos \psi - \cos \gamma)}}$$

en changeant simultanément α en $-\alpha$ et γ en $\pi - \gamma$. En faisant donc ce double changement dans l'expression de la somme de la première série, on trouve pour celle de la seconde:

$$\frac{1}{\sqrt{1 - 2\alpha \cos \gamma + \alpha^2}} = \frac{1}{2} R_0 + R_1 \alpha + R_2 \alpha^2 + \dots + R_n \alpha^n + \dots.$$

En ajoutant les deux séries, il vient:

$$\frac{1}{\sqrt{1 - 2\alpha \cos \gamma + \alpha^2}} = \frac{1}{2} P_0 + P_1 \alpha + P_2 \alpha^2 + \dots + P_n \alpha^n + \dots,$$

P_n désignant généralement l'expression (3), ce qu'il s'agissait de faire voir.

Pour vérifier l'équation (4), qui n'a pas lieu pour $n = 0$, considérons d'abord la série dont le terme général est le produit de α^n et de la première des intégrales qui y entrent. Ce terme général est:

$$-\frac{2}{\pi} \alpha^n \int_0^{\gamma} \frac{\sin n \psi \sin \frac{1}{2} \psi d\psi}{\sqrt{2(\cos \psi - \cos \gamma)}}.$$

En attribuant à n toutes les valeurs entières à partir de $n = 1$, et faisant la

somme, il viendra :

$$\begin{aligned} & -\frac{2}{\pi} \int_0^{\gamma} \frac{\sin \frac{1}{2} \psi d\psi}{\sqrt{2(\cos \psi - \cos \gamma)}} (\alpha \sin \psi + \alpha^2 \sin 2\psi + \dots) \\ &= -\frac{2}{\pi} \int_0^{\gamma} \frac{\sin \frac{1}{2} \psi d\psi}{\sqrt{2(\cos \psi - \cos \gamma)}} \cdot \frac{\alpha \sin \psi}{1 - 2\alpha \cos \psi + \alpha^2}. \end{aligned}$$

En remarquant que l'on a :

$$\frac{\alpha \sin \psi \sin \frac{1}{2} \psi}{1 - 2\alpha \cos \psi + \alpha^2} = \frac{1}{2} \cos \frac{1}{2} \psi - \frac{1}{2} \cdot \frac{(1-\alpha)^2 \cos \frac{1}{2} \psi}{1 - 2\alpha \cos \psi + \alpha^2}.$$

l'expression précédente devient :

$$-\frac{1}{\pi} \int_0^{\gamma} \frac{\cos \frac{1}{2} \psi d\psi}{\sqrt{2(\cos \psi - \cos \gamma)}} + \frac{(1-\alpha)^2}{\pi} \int_0^{\gamma} \frac{\cos \frac{1}{2} \psi d\psi}{\sqrt{2(\cos \psi - \cos \gamma)}} \cdot \frac{1}{1 - 2\alpha \cos \psi + \alpha^2}.$$

En mettant leurs valeurs pour ces deux intégrales dont la seconde s'est déjà présentée plus haut lorsqu'on a sommé la suite $\frac{1}{2}Q_1 + Q_1\alpha + \dots$, il viendra :

$$-\frac{1}{2} + \frac{1}{2} \frac{1-\alpha}{1 - 2\alpha \cos \gamma + \alpha^2}.$$

Si l'on considère en second lieu la série dont le terme général est égal à la seconde des intégrales (4) multipliée par α^n , on s'assurera, comme plus haut, que cette série résulte de celle qu'on vient de sommer, en changeant simultanément α en $-\alpha$ et γ en $\pi - \gamma$. Cette nouvelle série a donc pour somme :

$$-\frac{1}{2} + \frac{1}{2} \frac{1+\alpha}{1 - 2\alpha \cos \gamma + \alpha^2}.$$

En réunissant les deux résultats, on obtient cette égalité :

$$\frac{1}{1 - 2\alpha \cos \gamma + \alpha^2} - 1 = P_1\alpha + P_2\alpha^2 + \dots + P_n\alpha^n + \dots,$$

P_n étant donné par l'équation (4), qui se trouve ainsi vérifiée.

§. 2.

Après ces préliminaires, nous allons considérer la série :

$$(5) \quad \frac{1}{4\pi} \Sigma (2n+1) \int_0^{\pi} d\theta' \sin \theta' \int_0^{2\pi} P_n f(\theta', q') dq',$$

le signe sommatoire s'étendant à toutes les valeurs entières de n depuis zéro jusqu'à l'infini, et la fonction $f(\theta', q')$ étant donnée d'une manière arbitraire depuis $\theta' = 0, q' = 0$ jusqu'à $\theta' = \pi, q' = 2\pi$. On suppose seulement que cette fonction ne devient pas infinie entre ces limites. Quant à P_n , c'est le coefficient de a^n dans la valeur développée du radical:

$$\frac{1}{\sqrt{1 - 2a(\cos\theta\cos\theta' + \sin\theta\sin\theta'\cos(q'-q)) + a^2}}$$

On obtiendra ce coefficient, si l'on suppose:

$$\cos\gamma = \cos\theta\cos\theta' + \sin\theta\sin\theta'\cos(q'-q)$$

dans l'une des expressions de P_n obtenues dans le paragraphe précédent.

Pour sommer la suite (5), nous considérerons la somme de ses $n+1$ premiers termes, et nous montrerons que cette somme converge vers une limite lorsqu'on fait croître indéfiniment le nombre entier n . Supposons d'abord $\theta = 0$, cas auquel il sera très facile de ramener ensuite celui d'une valeur quelconque de cette variable. Cela étant, on aura $\cos\gamma = \cos\theta'$, et P_n ne contiendra pas la variable q' . Si l'on pose pour abrégier:

$$\frac{1}{2\pi} \int_0^{2\pi} f(\theta', q') dq' = F(\theta')$$

et que l'on écrive γ à la place de θ' , la somme des $n+1$ premiers termes de la série deviendra:

$$S = \frac{1}{2} \int_0^\pi [P_0 + 3P_1 + 5P_2 + \dots + (2n+1)P_n] F(\gamma) \sin\gamma d\gamma.$$

La lettre θ' ayant été remplacée par γ , les expressions de P_0, P_1, P_2, \dots seront celles qui résultent des équations (3) et (4), sans y rien changer.

La somme précédente peut être partagée en celles-ci:

$$T = \frac{1}{2} \int_0^\pi (P_0 + P_1 + P_2 + \dots + P_n) F(\gamma) \sin\gamma d\gamma,$$

$$U = \int_0^\pi (P_1 + 2P_2 + \dots + nP_n) F(\gamma) \sin\gamma d\gamma,$$

que nous examinerons l'une après l'autre. En introduisant dans la première les expressions de P_0, P_1, \dots, P_n données par l'équation (3) et ayant égard à

la formule connue :

$$1 + 2\cos\psi + 2\cos 2\psi + \dots + 2\cos n\psi = \frac{\sin\frac{1}{2}(2n+1)\psi}{\sin\frac{1}{2}\psi}.$$

il viendra :

$$T = \frac{1}{2\pi} \int_0^\pi dy F(y) \sin y \left(\int_0^\gamma \frac{\cos\frac{1}{2}\psi}{1 - 2(\cos\psi - \cos\gamma)} \cdot \frac{\sin\frac{1}{2}(2n+1)\psi d\psi}{\sin\frac{1}{2}\psi} \right. \\ \left. + \int_\gamma^\pi \frac{\sin\frac{1}{2}\psi}{1 - 2(\cos\gamma - \cos\psi)} \cdot \frac{\sin\frac{1}{2}(2n+1)\psi d\psi}{\sin\frac{1}{2}\psi} \right).$$

Quoique les intégrations relatives à ψ doivent être effectuées entre des limites dépendant de la variable γ , à laquelle se rapporte l'autre intégration, on peut facilement intervertir l'ordre des deux intégrations. Il suffit pour cela de faire usage de la formule suivante :

$$(6) \quad \int_0^a dx \int_0^c g(x, y) dy = \int_0^a dy \int_0^c g(x, y) dx.$$

qu'il est très facile de démontrer et qui devient tout à fait évidente, lorsqu'on l'envisage sous un point de vue géométrique. En effet, si l'on conçoit que x , y , $g(x, y)$ soient les coordonnées rectangulaires d'un point quelconque d'une surface courbe, on voit sur le champ que les intégrales précédentes représentent l'une et l'autre la partie de l'espace comprise entre cette surface, le plan des x , y et les trois plans perpendiculaires à ce dernier et dont les équations sont $y = 0$, $x = a$, et $y = c$.

On transformera la première partie de T , en l'assimilant au premier membre de l'égalité précédente et en remplaçant ce premier membre par le second, et l'on opérera en sens inverse pour la seconde partie de T . On trouve ainsi :

$$\tilde{T} = \frac{1}{2\pi} \int_0^\pi \frac{\sin\frac{1}{2}(2n+1)\psi}{\sin\frac{1}{2}\psi} H(\psi) d\psi, \quad ,$$

en posant pour abrégér :

$$H(\psi) = \cos\frac{1}{2}\psi \int_0^\pi \frac{F(\gamma) \sin\gamma d\gamma}{1 - 2(\cos\psi - \cos\gamma)} + \sin\frac{1}{2}\psi \int_0^\pi \frac{F(\gamma) \sin\gamma d\gamma}{1 - 2(\cos\gamma - \cos\psi)}.$$

$H(\psi)$ sera une fonction de ψ qui reste finie pour toute valeur de ψ comprise entre 0 et π . En effet, si l'on désigne par M , abstraction faite du signe, la plus grande valeur de $F(\gamma)$ depuis $\gamma = 0$ jusqu'à $\gamma = \pi$, il est évident que la

valeur numérique de l'intégrale:

$$\int_{\psi}^{\pi} \frac{F(\gamma) \sin \gamma d\gamma}{\sqrt{2(\cos \psi - \cos \gamma)}}$$

est moindre que:

$$M \int_{\psi}^{\pi} \frac{\sin \gamma d\gamma}{\sqrt{2(\cos \psi - \cos \gamma)}} = 2M \cos \frac{1}{2} \psi.$$

L'autre intégrale est inférieure à $2M \sin \frac{1}{2} \psi$ et par conséquent $\mathbf{H}(\psi)$ moindre que $2M$.

La fonction $\mathbf{H}(\psi)$ ne devenant pas infinie, on déterminera facilement la limite vers laquelle T converge, au moyen d'un théorème qui se présente dans la théorie des séries de sinus et de cosinus. En posant $\psi = 2\beta$, il viendra:

$$T = \frac{1}{\pi} \int_0^{\pi} \frac{\sin(2n+1)\beta}{\sin \beta} \mathbf{H}(2\beta) d\beta$$

et l'on conclura immédiatement de ce théorème (Voyez la note à la fin du Mémoire) que la limite de T pour des valeurs de n indéfiniment croissantes est égale à $\frac{1}{2} \mathbf{H}(0)$. En ayant égard à ce que $\mathbf{H}(\psi)$ représente, on trouve:

$$\mathbf{H}(0) = \int_0^{\pi} F(\gamma) \cos \frac{1}{2} \gamma d\gamma.$$

La limite vers laquelle T converge, est donc $\frac{1}{2} \int_0^{\pi} F(\gamma) \cos \frac{1}{2} \gamma d\gamma$.

§. 3.

Passons maintenant à la considération de U . En y mettant pour P_1, P_2, \dots, P_n les expressions que fournit l'équation (4), et intervertissant ensuite l'ordre des intégrations au moyen de la formule (6), on aura:

$$(7) \quad U = \frac{2}{\pi} \int_0^{\pi} \Theta(\psi) (\sin \psi + 2 \sin 2\psi + \dots + n \sin n\psi) d\psi,$$

en posant pour abrégér:

$$\Theta(\psi) = -\sin \frac{1}{2} \psi \int_{\psi}^{\pi} \frac{F(\gamma) \sin \gamma d\gamma}{\sqrt{2(\cos \psi - \cos \gamma)}} + \cos \frac{1}{2} \psi \int_0^{\psi} \frac{F(\gamma) \sin \gamma d\gamma}{\sqrt{2(\cos \gamma - \cos \psi)}}.$$

Les deux intégrales que renferme $\Theta(\psi)$, étant les mêmes que celles qui entrent dans $\mathbf{H}(\psi)$, on conclut comme précédemment que la fonction $\Theta(\psi)$ ne devient pas infinie. Mais il faut prouver de plus que $\Theta(\psi)$ est une fonction continue, c'est-à-dire qui change par degrés insensibles lorsqu'on fait croître ψ d'une

manière semblable, depuis $\psi = 0$ jusqu'à $\psi = \pi$. Cette propriété a lieu quand même la fonction $F(\gamma)$ qui entre dans la composition de $\Theta(\psi)$, serait discontinue, c'est-à-dire quand même la courbe dont γ est l'abscisse et $F(\gamma)$ l'ordonnée, serait composée de parties non contigües. Il est toujours bien entendu que $F(\gamma)$ doit rester finie, condition qui est évidemment remplie dès qu'elle a lieu pour la fonction $f(\theta, \gamma')$ dont $F(\gamma)$ dérive. La même propriété appartient aussi à $\Pi(\psi)$, mais il n'était pas nécessaire d'y avoir égard dans l'examen que nous avons fait de T .

Pour prouver la propriété énoncée, il suffit évidemment de faire voir que cette propriété convient à chacune des intégrales que renferme $\Theta(\psi)$. Si l'on suppose que dans la seconde de ces deux intégrales, ψ augmente de la quantité positive ε , l'intégrale augmentera de :

$$\int_0^{\psi+\varepsilon} \frac{F(\gamma)\sin\gamma d\gamma}{\sqrt{2(\cos\gamma - \cos(\psi+\varepsilon))}} - \int_0^{\psi} \frac{F(\gamma)\sin\gamma d\gamma}{\sqrt{2(\cos\gamma - \cos\psi)}}.$$

Cette différence peut être mise sous cette forme :

$$- \int_0^{\psi} F(\gamma) \left[\frac{\sin\gamma}{\sqrt{2(\cos\gamma - \cos\psi)}} - \frac{\sin\gamma}{\sqrt{2(\cos\gamma - \cos(\psi+\varepsilon))}} \right] d\gamma + \int_{\psi}^{\psi+\varepsilon} \frac{F(\gamma)\sin\gamma d\gamma}{\sqrt{2(\cos\gamma - \cos(\psi+\varepsilon))}}.$$

Comme le facteur de $F(\gamma)$, dans la première de ces deux intégrales, reste évidemment toujours positif entre les limites de l'intégration, il est évident que l'intégrale est moindre, abstraction faite du signe, que l'intégrale de ce facteur prise entre les mêmes limites, multipliée par la plus grande valeur de $F(\gamma)$, que nous désignerons par M comme plus haut.

L'intégration étant effectuée, on trouve pour la quantité que la valeur numérique de l'intégrale ne saurait surpasser :

$$2M[\sin \frac{1}{2}\psi - \sin \frac{1}{2}(\psi - \varepsilon) + \sqrt{\sin \frac{1}{2}\varepsilon \sin(\psi + \frac{1}{2}\varepsilon)}].$$

On trouve pareillement que la valeur numérique de la seconde intégrale est inférieure à :

$$2M\sqrt{\sin \frac{1}{2}\varepsilon \sin(\psi + \frac{1}{2}\varepsilon)}.$$

Les expressions précédentes s'évanouissant avec ε , il en résulte que l'accroissement de l'intégrale :

$$\int_0^{\psi} \frac{F(\gamma)\sin\gamma d\gamma}{\sqrt{2(\cos\gamma - \cos\psi)}},$$

correspondant à une augmentation infiniment petite de la variable ψ , est lui-

même une quantité infiniment petite. Cette intégrale sera donc une fonction continue de ψ .

Le même raisonnement s'appliquant à l'autre intégrale que renferme $\Theta(\psi)$, la continuité de cette fonction se trouve établie.

Il est évident, à la seule inspection de l'expression de cette fonction, qu'elle s'évanouit aux deux limites $\psi = 0$ et $\psi = \pi$, c'est-à-dire que l'on a ces deux équations:

$$(8) \quad \Theta(0) = 0, \quad \Theta(\pi) = 0.$$

Posons pour abrégier $\frac{d\Theta(\psi)}{d\psi} = \Theta'(\psi)$, et voyons quelle est la valeur de $\Theta'(\psi)$, lorsque ψ obtient la valeur particulière 0. Si l'on désigne, pour un instant, par r et s les deux intégrales contenues dans $\Theta(\psi)$, on aura:

$$\Theta(\psi) = -r \sin \frac{1}{2} \psi + s \cos \frac{1}{2} \psi,$$

et en différentiant:

$$\Theta'(\psi) = -\frac{1}{2} r \cos \frac{1}{2} \psi - \frac{1}{2} s \sin \frac{1}{2} \psi - \frac{dr}{d\psi} \sin \frac{1}{2} \psi + \frac{ds}{d\psi} \cos \frac{1}{2} \psi.$$

Pour $\psi = 0$, on a évidemment:

$$r = \int_0^{\frac{\pi}{2}} F(\gamma) \cos \frac{1}{2} \gamma d\gamma, \quad s = 0.$$

Pour déterminer $\frac{ds}{d\psi}$ dans ce même cas, on remarquera qu'à cause de $s = 0$,

$\frac{ds}{d\psi}$ est évidemment la limite du rapport:

$$\frac{1}{\varepsilon} \int_0^{\varepsilon} F(\gamma) \sin \gamma d\gamma$$

la quantité positive ε décroissant indéfiniment. Ce rapport est compris entre les deux quantités:

$$\frac{g}{\varepsilon} \int_0^{\varepsilon} \frac{\sin \gamma d\gamma}{\sqrt{2(\cos \gamma - \cos \varepsilon)}} \quad \text{et} \quad \frac{h}{\varepsilon} \int_0^{\varepsilon} \frac{\sin \gamma d\gamma}{\sqrt{2(\cos \gamma - \cos \varepsilon)}}.$$

ou ce qui revient au même, entre celles-ci:

$$g \frac{\sin \frac{1}{2} \varepsilon}{\frac{1}{2} \varepsilon} \quad \text{et} \quad h \frac{\sin \frac{1}{2} \varepsilon}{\frac{1}{2} \varepsilon}.$$

g et h désignant les valeurs extrêmes de $F(\gamma)$ dans l'intervalle de l'intégration. Les expressions précédentes convergeant vers la limite $F(0)$, on aura $\frac{ds}{d\psi} = F(0)$, pour la valeur particulière $\psi = 0$. On trouverait d'une manière semblable, la valeur de $\frac{dr}{d\psi}$ correspondant à $\psi = 0$, valeur dont on n'a toutefois besoin que pour s'assurer qu'elle ne peut pas être infinie. Au moyen des détermina-

tions précédentes, on conclut :

$$(9) \quad \Theta'(0) = F(0) - \frac{1}{2} \int_0^{\pi} F(\gamma) \cos \frac{1}{2} \gamma d\gamma.$$

Cela posé, reprenons l'expression de U' (7). La suite :

$$\sin \psi + 2 \sin 2\psi + \dots + n \sin n\psi$$

étant mise sous la forme :

$$- \frac{d}{d\psi} \left(\frac{1}{2} + \cos \psi + \cos 2\psi + \dots + \cos n\psi \right) = - \frac{1}{2} \frac{d}{d\psi} \frac{\sin(2n+1)\frac{1}{2}\psi}{\sin \frac{1}{2}\psi},$$

on aura :

$$U = - \frac{1}{\pi} \int_0^{\pi} \Theta(\psi) \frac{d}{d\psi} \frac{\sin(2n+1)\frac{1}{2}\psi}{\sin \frac{1}{2}\psi} d\psi.$$

En intégrant par parties, on trouve :

$$U = \frac{1}{\pi} \int_0^{\pi} \Theta'(\psi) \frac{\sin(2n+1)\frac{1}{2}\psi}{\sin \frac{1}{2}\psi} d\psi,$$

le terme :

$$- \Theta(\psi) \frac{\sin(2n+1)\frac{1}{2}\psi}{\sin \frac{1}{2}\psi}$$

que cette opération fait sortir du signe, disparaissant. Cela résulte 1^o des deux équations (8) d'après lesquelles $\Theta(\psi)$ s'évanouit aux limites, et 2^o de ce que cette fonction $\Theta(\psi)$ reste continue dans toute l'étendue de l'intégration, comme nous l'avons fait voir plus haut.

Sous cette forme il est évident par le théorème déjà cité (Voyez la note à la fin du Mémoire) que U converge vers la limite $\Theta'(0)$, ou ce qui revient au même d'après l'équation (9), vers la limite :

$$F(0) - \frac{1}{2} \int_0^{\pi} F(\gamma) \cos \frac{1}{2} \gamma d\gamma.$$

Il est essentiel de remarquer que ce résultat ne cesse pas d'être exact, quand même la fonction $\Theta'(\psi)$ deviendrait infinie pour certaines valeurs particulières de ψ . Quoique $\Theta(\psi)$ conserve toujours une valeur finie, la même propriété ne convient pas toujours à la fonction dérivée $\Theta'(\psi)$. Il serait au contraire facile de s'assurer que $\Theta'(\psi)$ devient nécessairement infinie pour certaines valeurs particulières de la variable ψ , toutes les fois que la fonction $F(\gamma)$, dont $\Theta(\psi)$ dépend, est une fonction discontinue.

Mais, comme on l'a déjà dit, cette circonstance n'empêchera pas le théorème de la note d'être applicable, la condition que ce théorème exige, et qui consiste en ce que l'intégrale $\int_0^{\pi} \Theta'(\psi) d\psi = \Theta(\psi)$ doit rester finie, étant évidemment remplie.

En réunissant les résultats qu'on vient d'obtenir, on conclura que la somme $S = T + U$ converge vers la limite $F(0)$ pour des valeurs croissantes de n . Il suit de là que la série (5), lorsqu'on y suppose $\theta = 0$, est convergente et a pour somme $F(0)$, et comme l'on a posé plus haut:

$$F(\theta) = \frac{1}{2\pi} \int_0^{2\pi} f(\theta', q') dq',$$

cette somme sera donnée par l'intégrale $\frac{1}{2\pi} \int_0^{2\pi} f(0, q') dq'$.

§. 4.

Pour passer plus facilement au cas général, où l'on attribue dans la série (5), à θ et q des valeurs quelconques, il convient de présenter sous une forme géométrique le résultat auquel on vient de parvenir. Pour cela, concevons une surface sphérique d'un rayon égal à l'unité. Si par un point fixe de cette surface on fait passer un arc de grand cercle, que nous considérons également comme fixe et prolongé d'un seul côté, la position d'un point quelconque de cette surface sera déterminée dès que l'on connaîtra l'arc de grand cercle compris entre ce point et le point fixe, et l'angle sphérique que cet arc forme avec l'arc fixe. Ces deux coordonnées polaires sphériques étant désignées par θ' et q' , on embrassera évidemment la surface entière, en attribuant à θ' toutes les valeurs comprises entre $\theta' = 0$ et $\theta' = \pi$, et à q' toutes celles comprises entre $q' = 0$ et $q' = 2\pi$, et il est également évident que l'élément de surface relatif à ces coordonnées, sera exprimé par $\sin\theta' d\theta' dq'$. La fonction $f(\theta', q')$ étant ainsi donnée pour la surface entière, on voit que l'intégrale:

$$F(\theta) = \frac{1}{2\pi} \int_0^{2\pi} f(\theta', q') dq'$$

est la moyenne de toutes les valeurs de cette fonction correspondant aux différents points de la circonférence d'un petit cercle, décrit de l'origine comme centre et avec un rayon sphérique égal à θ' . Si la fonction $f(\theta', q')$ devient indépendante de l'angle q' , lorsqu'on y fait $\theta' = 0$, on aura:

$$F(0) = \frac{1}{2\pi} \int_0^{2\pi} f(0, q') dq' = f(0, q'),$$

et la somme de la série (5) coïncidera avec la valeur de la fonction relative à l'origine des coordonnées. Mais dans le cas général où la supposition de $\theta' = 0$ ne fait pas disparaître q' , la fonction $f(\theta', q')$ aura une infinité de valeurs différentes à cette origine et sera discontinue dans tous les sens autour

de ce point. La somme de la série étant toujours exprimée par $\frac{1}{2\pi} \int_0^{2\pi} f(\theta, q') dq'$, sera alors la moyenne de toutes ces valeurs en nombre infini. On peut donc dire généralement que la série (5), lorsqu'on y pose $\theta = 0$, a pour somme la moyenne de toutes les valeurs de $f(\theta, q')$ qui ont lieu sur la circonférence d'un cercle infiniment petit et dont le centre est à l'origine des coordonnées.

Pour passer du cas où $\theta = 0$, à celui où θ et q sont quelconques mais inférieures à π et à 2π , on pourrait transporter l'origine au point dont les coordonnées sphériques sont θ et q . Mais on peut se dispenser de ce calcul, en examinant attentivement le terme général dans l'un et dans l'autre cas.

Dans les deux cas le terme général est exprimé par une intégrale double étendue à toute la surface sphérique, et dont l'élément est le produit de deux facteurs. Le premier:

$$f(\theta', q') \sin \theta' d\theta' dq'$$

exprimant l'élément de surface multiplié par la valeur de $f(\theta', q')$ qui s'y rapporte, est le même dans les deux cas et il n'y a de différence que pour l'autre facteur P_n . Dans le premier cas, ce facteur P_n est une certaine fonction de la distance sphérique θ' de l'élément de surface à l'origine des coordonnées, et dans le second cas, P_n est la même fonction de γ , γ étant donnée par l'équation:

$$\cos \gamma = \cos \theta \cos \theta' + \sin \theta \sin \theta' \cos(q' - q).$$

Or on sait, par la trigonométrie, que γ est la distance des deux points ayant pour coordonnées θ, q et θ', q' , il est donc évident que les deux cas ne se distinguent qu'en ce que l'origine des distances qui coïncide avec celle des coordonnées dans le premier cas, se trouve dans le second au point quelconque (θ, q) . On voit donc que la série est de même nature dans l'un et l'autre cas, et comme on a prouvé la convergence de cette série pour le premier cas, en même temps qu'on en a obtenu la somme, on peut transporter au cas général le résultat trouvé plus haut. On trouve ainsi que la série (5) est une série convergente, et dont la somme est exprimée par la moyenne de toutes les valeurs de la fonction $f(\theta', q')$, relatives aux différents points du contour d'un cercle infiniment petit ayant son centre au point (θ, q) . Cet énoncé embrasse tous les cas.

Lorsque le point (θ, q) n'est pas du nombre de ceux autour desquels la fonction arbitrairement donnée pour toute l'étendue de la surface sphérique est discontinue, la moyenne précédente coïncidera avec $f(\theta, q)$, qui est alors la somme de la série (5), ce qu'il s'agissait de faire voir.

Pour éclaircir cet énoncé par un exemple très simple, concevons qu'après avoir tracé un polygone sphérique quelconque, on suppose la fonction arbitraire $f(\theta, \varphi)$ égale à l'unité pour tous les points dans l'intérieur du polygone et égale à zéro pour les points extérieurs. Il faudra donc remplacer, dans la série (5), $f(\theta, \varphi)$ par l'unité et n'étendre ensuite la double intégration qu'à la surface du polygone. Les termes de la série étant ainsi complètement déterminés, si l'on substitue dans cette série des valeurs quelconques θ et φ , la valeur correspondante de la série sera l'unité ou zéro, selon que le point dont les coordonnées sont θ, φ , sera situé en dedans ou en dehors du polygone. Dans le cas intermédiaire où le point (θ, φ) appartiendra au contour du polygone, la moyenne de toutes les valeurs de $f(\theta, \varphi)$ correspondant aux différents points du contour du cercle infiniment petit, sera évidemment $\frac{1}{2}$, valeur qui sera donc aussi celle de la série. Mais ce résultat cesse lui-même d'être exact, lorsque le point (θ, φ) appartient à la fois à deux parties différentes du contour, c'est-à-dire lorsque les coordonnées θ, φ sont celles d'un sommet du polygone, et il résulte de l'énoncé général qu'alors la somme de la série est égale à l'angle auquel ce sommet appartient, divisé par quatre droits.

§. 5.

Après avoir prouvé qu'une fonction $f(\theta, \varphi)$, arbitrairement donnée depuis $\theta = 0, \varphi = 0$ jusqu'à $\theta = \pi, \varphi = 2\pi$, peut être exprimée par une série convergente dont le terme général X_n est une expression rationnelle et entière du degré n , des quantités $\cos\theta, \sin\theta\cos\varphi, \sin\theta\sin\varphi$, telle que l'équation (c) soit satisfaite, il nous reste à faire voir que la même fonction n'est susceptible que d'un seul développement de cette espèce. Il suffit pour cela de prouver, que, si Y_m est une expression de même nature que X_n et du degré m , on a toujours*):

$$(d) \quad \iint X_n Y_m \sin\theta d\theta d\varphi = 0.$$

les intégrations s'étendant depuis $\theta = 0, \varphi = 0$ jusqu'à $\theta = \pi, \varphi = 2\pi$, et les indices n et m étant supposés différents. Si, après avoir remplacé dans l'intégrale précédente X_n par les deux termes qui sont équivalents à cette expression en vertu de l'équation (c), on chasse, au moyen de l'intégration par parties, les coefficients différentiels qui sont ainsi introduits, et que l'on ait ensuite égard à l'équation aux différences partielles à laquelle Y_m est supposé

*) Mécanique céleste. Tome II, p. 31.

satisfaisant, il viendra :

$$[n(n+1) - m(m+1)] \iiint X_n Y_m \sin \theta d\theta d\varphi = 0,$$

résultat qui coïncide avec l'équation (d).

Cela posé, si la fonction $f(\theta, \varphi)$, qu'on suppose complètement donnée pour toutes les valeurs de θ et de φ comprises entre $\theta = 0$, $\varphi = 0$ et $\theta = \pi$, $\varphi = 2\pi$, était susceptible de deux développements différents, on aurait entre ces limites :

$$Y_n + Y_1 + Y_2 + \dots + Y_n + \dots = Z_0 + Z_1 + Z_2 + \dots + Z_n + \dots,$$

Z_n désignant une expression de même nature que Y_n . En posant $X_n = Y_n - Z_n$, X_n sera évidemment encore de même nature, et l'on conclut :

$$X_n + X_1 + X_2 + \dots + X_n + \dots = 0.$$

Cette égalité ayant lieu entre les limites indiquées, si on l'intègre entre ces mêmes limites après l'avoir multipliée par $X_n \sin \theta d\theta d\varphi$, tous les termes, à l'exception d'un seul, disparaîtront en vertu de l'équation (d), et il viendra :

$$\iint X_n^2 \sin \theta d\theta d\varphi = 0,$$

d'où suit qu'on a identiquement $X_n = 0$, ce qu'il s'agissait de prouver.

Il n'est peut-être pas inutile de faire remarquer que la propriété importante qu'on vient de rappeler, n'est pas particulière aux séries dont les termes généraux satisfont à l'équation (c), comme on a paru le croire. Elle convient, au contraire, à toute autre forme de développement propre à exprimer une fonction arbitraire. Les termes d'un pareil développement sont toujours complètement déterminés, lorsque la fonction est donnée dans toute l'étendue de l'intervalle pour lequel elle peut être choisie à volonté. C'est ainsi, par exemple, qu'une fonction $f(x)$ donnée depuis $x = 0$ jusqu'à $x = \pi$, n'est susceptible que d'un seul développement de la forme :

$$a_1 \sin x + a_2 \sin 2x + \dots + a_n \sin nx + \dots,$$

et l'on a nécessairement $a_n = \frac{2}{\pi} \int_0^\pi \sin nx f(x) dx$.

Comme P_n considéré par rapport aux variables θ, φ , est de même nature que X_n , on aura en vertu de l'équation (d) :

$$\iint P_n Y_m \sin \theta d\theta d\varphi = 0,$$

n étant toujours supposé différent de m . Soit Y'_m ce que Y_m devient lorsqu'on y remplace θ, φ par θ', φ' ; l'équation précédente donnera en y mettant θ', φ'

à la place de θ , q , et réciproquement, ce qui ne change rien au coefficient P_m :

$$\iint P_m Y_m \sin \theta' d\theta' dq' = 0.$$

Cela posé, si l'on suppose que, dans l'équation (a), la fonction $f(\theta, q)$ se réduise à Y_m , tous les termes du second membre, à l'exception de celui dont l'indice est m , s'évanouiront en vertu de l'équation précédente et l'on obtient:

$$(c) \quad Y_m = \frac{2m+1}{4\pi} \int_0^\pi d\theta' \sin \theta' \int_0^{2\pi} P_m Y_m' dq'.$$

résultat remarquable et qu'on a souvent occasion d'employer.

Addition au Mémoire précédent.

On a ces deux théorèmes:

„La fonction $f(\beta)$ restant finie depuis $\beta = 0$ jusqu'à $\beta = h$ (où $0 < h < \frac{1}{2}\pi$), l'intégrale $\int_0^h f(\beta) \frac{\sin k\beta}{\sin \beta} d\beta$ convergera vers $\frac{1}{2}\pi f(0)$, si la quantité positive k devient infinie.“

„La fonction $f(\beta)$ restant finie depuis $\beta = g$ jusqu'à $\beta = h$, (où $0 < g < h < \frac{1}{2}\pi$), l'intégrale $\int_g^h f(\beta) \frac{\sin k\beta}{\sin \beta} d\beta$ s'évanouira pour $k = \infty$.“

Ces deux théorèmes dont le premier est celui dont nous avons fait usage dans le Mémoire précédent, se démontrent d'une manière très simple lorsqu'on suppose d'abord que la fonction $f(\beta)$ reste continue et toujours croissante ou toujours décroissante entre les limites des intégrations*), et que l'on passe ensuite au cas général où cette fonction serait discontinue et alternativement croissante et décroissante entre ces limites, en décomposant les intégrales en d'autres entre les limites desquelles ni l'une ni l'autre de ces circonstances n'a plus lieu et dont les valeurs correspondant à $k = \infty$, résulteront par conséquent immédiatement du premier cas.

Pour que l'analyse par laquelle nous avons déterminé la limite de l'expression U (§. 3), soit complète, il est essentiel de remarquer que le premier des théorèmes précédents ne cesse pas d'être exact quand même la fonction $f(\beta)$ deviendrait infinie pour une ou pour plusieurs valeurs de β différentes de zéro et comprises entre $\beta = 0$ et $\beta = h$, pourvu qu'alors l'intégrale $\int_0^h f(\beta) d\beta = F(\beta)$ reste finie et continue depuis $\beta = 0$ jusqu'à $\beta = h$.

*) Journal de CRELLE, Vol. IV, p. 165. 1)

1) S. 128 dieser Ausgabe von G. Lejeune Dirichlet's Werken. — K.

Pour nous en assurer, supposons que $f(\beta')$ ne devienne infinie que pour $\beta = c$, le même raisonnement s'étendant sans difficulté au cas d'un plus grand nombre de valeurs. Désignons par ε une quantité positive que nous supposons invariable tandis que k croît au-delà de toute limite, et décomposons l'intégrale $\int_0^h f(\beta) \frac{\sin k\beta}{\sin \beta} d\beta$ en quatre autres, ayant respectivement pour limites:

$$0 \text{ et } c-\varepsilon, \quad c-\varepsilon \text{ et } c, \quad c \text{ et } c+\varepsilon, \quad c+\varepsilon \text{ et } h.$$

La fonction $f(\beta')$ ne devenant pas infinie entre les limites de la première et de la quatrième de ces nouvelles intégrales, ces intégrales deviendront respectivement $\frac{1}{2}\pi f(0)$ et 0, pour $k = \infty$. Quant aux deux autres, on remarquera que la quantité arbitraire ε peut être choisie assez petite pour que $f(\beta)$ conserve toujours le même signe depuis $\beta = c-\varepsilon$ jusqu'à $\beta = c$, et qu'il en soit de même pour l'intervalle compris entre $\beta = c$ et $\beta = c+\varepsilon$, ce dernier signe pouvant d'ailleurs être différent du premier, puisque $f(\beta')$ peut changer de signe en passant par l'infini.

(Cela aurait lieu par exemple si l'on avait $f(\beta) = -\frac{1}{2\sqrt{c-\beta}}$, tant que $\beta < c$, et $f(\beta) = \frac{1}{2\sqrt{\beta-c}}$, lorsque $\beta > c$. Dans ce cas, $F(\beta)$ serait $\sqrt{c-\beta} - \sqrt{c}$ ou $\sqrt{\beta-c} - \sqrt{c}$ selon que $\beta < c$ ou $\beta > c$, et remplirait par conséquent la condition énoncée plus haut, les expressions précédentes étant des fonctions continues de β et coïncidant pour $\beta = c$.)

Cela posé, il est évident que la seconde et la troisième intégrale seront, abstraction faite du signe, et quel que soit k , respectivement inférieures aux quantités:

$$\frac{F(c) - F(c-\varepsilon)}{\sin(c-\varepsilon)}, \quad \frac{F(c+\varepsilon) - F(c)}{\sin c}.$$

Comme $F(\beta)$ est, par hypothèse, une fonction continue de β , et comme c diffère de zéro et de tout autre multiple de π (puisque l'on a $c < \frac{1}{2}\pi$), on voit que les valeurs précédentes peuvent devenir moindres que toute grandeur donnée, en choisissant ε suffisamment petit.

Mais on a vu, d'un autre côté, que quelque petit que l'on suppose la quantité invariable ε , la somme des deux autres intégrales convergera toujours pour des valeurs croissantes de k , vers la limite $\frac{1}{2}\pi f(0)$, limite qui sera donc aussi celle de l'intégrale $\int_0^h f(\beta) \frac{\sin k\beta}{\sin \beta} d\beta$, pour $k = \infty$, ce qu'il s'agissait de prouver.

Beweis eines Satzes
Ueber die arithmetische Progression.

VON

G. LEJEUNE DIRICHLET.

Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1837, S. 108—110.

BEWEIS EINES SATZES UEBER DIE ARITHMETISCHE PROGRESSION.

[Auszug aus einer in der Akademie der Wissenschaften am 27. Juli 1837 gelesenen Abhandlung „über den Satz, dass jede arithmetische Progression, deren erstes Glied und Differenz keinen gemeinschaftlichen Factor haben, unendlich viele Primzahlen enthält.“]

Es existirte bisher kein strenger Beweis des Satzes,

dass jede arithmetische Progression, deren erstes Glied und Differenz keinen gemeinschaftlichen Factor haben, unendlich viele Primzahlen enthält.

Dieser Satz ist aber für die höhere Arithmetik nicht ohne Wichtigkeit, nicht nur weil derselbe bei verschiedenen Untersuchungen als Lemma benutzt werden kann, sondern auch weil derselbe als das Complement einer der schönsten Theorien dieses Theiles der Wissenschaft anzusehen ist, der Lehre nämlich von den Linearformen der einfachen Divisoren der quadratischen Ausdrücke. Wird z. B. aus dem Fundamentalsatze dieser Lehre, dem sogenannten Reciprocitätsgesetze, gefolgert, dass der Ausdruck x^2+7 alle Primzahlen der drei Formen $7n+1$, $7n+2$, $7n+4$ und nur diese zu Divisoren hat, so bleibt ganz unentschieden, wie diese einfachen Divisoren unter jene Formen vertheilt sind. So lange der oben erwähnte Satz nicht bewiesen ist, wäre es denkbar, dass eine oder zwei der genannten Formen gar keine Primzahlen enthielten.

Was nun den Beweis des Satzes über die arithmetische Progression betrifft, so kann von demselben hier nur eine kurze Andeutung für den Fall gegeben werden, wo die Differenz der Progression eine ungerade Primzahl p ist. Für diesen Fall gestaltet sich der Beweis, der eine gewisse Analogie mit den

von EULER in dem Capitel *de seriebus ex evolutione productorum ortis* seiner *Introductio in analysin infinitorum* entwickelten Betrachtungen darbietet*), dem Wesentlichen nach wie folgt:

Ist a eine primitive Wurzel der Primzahl p , so fallen die Reste:

$$a_0, a_1, a_2, \dots, a_{p-2}$$

der Potenzen:

$$a^0, a^1, a^2, \dots, a^{p-2},$$

wenn man von der Ordnung absieht, mit den Zahlen:

$$1, 2, 3, \dots, p-1$$

zusammen, und der Beweis des erwähnten Satzes erfordert für diesen Fall die Nachweisung, dass jede der $p-1$ Formen:

$$np+a_0, np+a_1, np+a_2, \dots, np+a_{p-2}$$

unendlich viele Primzahlen enthält.

Es sei q irgend eine von p verschiedene Primzahl, deren Index μ heisse, so dass also:

$$a^\mu \equiv q \pmod{p}.$$

es sei ferner ω eine Wurzel der Gleichung:

$$(1) \quad \omega^{p-1} - 1 = 0,$$

und man bilde die geometrische Reihe:

$$\frac{1}{1-\omega^a} = 1 + \omega^a + \omega^{2a} + \omega^{3a} + \dots,$$

in welcher s positiv und grösser als Eins ist. Multipliziert man die ähnlichen Gleichungen, welche allen q , d. h. allen Primzahlen, mit Ausnahme der einzigen p entsprechen, in einander, nimmt dann die natürlichen Logarithmen von beiden Seiten und entwickelt endlich die Logarithmen auf der ersten Seite nach Potenzen von ω , indem man nach (1) die Vielfachen von $p-1$ in den Exponenten dieser Potenzen überall weglässt, so kommt:

$$G_0 + H_0 + (G_1 + H_1)\omega + \dots + (G_{p-2} + H_{p-2})\omega^{p-2} = \log L,$$

wo L die unendliche Reihe:

*) Band I, Cap. XV.

$$\sum_{n=0}^{n=\infty} \left(\frac{1}{(np+1)^s} + \frac{1}{(np+a_1)^s} \omega + \dots + \frac{1}{(np+a_{p-2})^s} \omega^{p-2} \right),$$

G_m die Summe der zur Potenz $-s$ erhobenen Primzahlen der Form $np+a_m$ bezeichnet, und auch das Bildungsgesetz von H_m leicht zu erkennen ist. Diese Gleichung gilt für alle Wurzeln der Gleichung (1), welche Wurzeln bekanntlich, wenn ω gehörig gewählt ist, durch:

$$1, \omega, \omega^2, \dots, \omega^{p-2}$$

dargestellt werden können, und repräsentirt also $p-1$ besondere, diesen Wurzeln entsprechende Gleichungen.

Entwickelt man $G_m + H_m$ aus diesen Gleichungen, so erhält man:

$$G_m + H_m = \frac{1}{p-1} (\log L_0 + \omega^{-m} \log L_1 + \omega^{-2m} \log L_2 + \dots + \omega^{-(p-2)m} \log L_{p-2}),$$

wo:

$$L_0, L_1, \dots, L_{p-2}$$

die den Wurzeln:

$$1, \omega, \dots, \omega^{p-2}$$

entsprechenden Werthe von L bezeichnen.

Lässt man jetzt s abnehmen und sich der Einheit ins Unendliche nähern, so wächst L_0 und also auch $\log L_0$ über alle Grenzen, während sich:

$$L_1, L_2, \dots, L_{p-2}$$

endlichen Grenzen nähern. Es werden also auch:

$$\log L_1, \log L_2, \dots, \log L_{p-2}$$

für $s = 1$ endlich bleiben, wenn die Werthe, welche:

$$L_1, L_2, \dots, L_{p-2}$$

für $s = 1$ annehmen, alle von Null verschieden sind. Dass dieses der Fall ist, lässt sich für alle leicht zeigen, mit Ausnahme von $L_{\frac{p-1}{2}}$, der eine ausführliche Untersuchung erfordert. Man findet durch dieselbe, dass der Grenzwert von $L_{\frac{p-1}{2}}$, wenn p die Form $4\nu+3$ hat, durch:

$$\frac{\pi}{p\sqrt{p}} (B-A)$$

ausgedrückt ist, wo π die halbe Peripherie für den Radius *Ein*s und A, B respective die Summe der quadratischen Reste und Nicht-Reste von p bezeichnen.

welche kleiner als p sind, und man beweist leicht, dass immer $B > A$. Ist p von der Form $4\nu+1$, so wird der Grenzwert von $L_{\frac{p-1}{2}}$, der auch in diesem Falle von Null verschieden ist, durch einen Logarithmus gegeben, und hängt mit den kleinsten Zahlen g, h zusammen, welche der Gleichung $g^2 - ph^2 = 1$ genügen.

Da hiernach, wenn sich s der Einheit nähert, bloss das erste Glied $\log L_0$ der zweiten Seite, und also die ganze zweite Seite der vorigen Gleichung über alle Grenzen hinaus wächst, so wird auch die erste Seite $G_m + H_m$ für $s = 1$ unendlich. Man überzeugt sich aber leicht, dass H_m in diesem Falle endlich bleibt, woraus dann sogleich folgt, dass die Summe der reciproken Primzahlen der Form $np + \sigma_m$ unendlich ist, und dass folglich in dieser Form unendlich viele Primzahlen enthalten sind.

BEWEIS DES SATZES, DASS JEDE UNBEGRENZTE
ARITHMETISCHE PROGRESSION, DEREN ERSTES
GLIED UND DIFFERENZ GANZE ZAHLEN
OHNE GEMEINSCHAFTLICHEN FACTOR SIND,
UNENDLICH VIELE PRIMZAHLEN ENTHÄLT.

VON

G. LEJEUNE DIRICHLET.

Abhandlungen der Königlich Preussischen Akademie der Wissenschaften von 1837, S. 45 — 81.

BEWEIS DES SATZES,
DASS JEDE UNBEGRENZTE ARITHMETISCHE PROGRESSION,
DEREN ERSTES GLIED UND DIFFERENZ GANZE ZAHLEN OHNE
GEMEINSCHAFTLICHEN FACTOR SIND, UNENDLICH VIELE
PRIMZAHLEN ENTHÄLT.

[Gelesen in der Akademie der Wissenschaften am 27. Juli 1837.]

Die aufmerksame Betrachtung der natürlichen Reihe der Primzahlen lässt an derselben eine Menge von Eigenschaften wahrnehmen, deren Allgemeinheit durch fortgesetzte Induction zu jedem beliebigen Grade von Wahrscheinlichkeit erhoben werden kann, während die Auffindung eines Beweises, der allen Anforderungen der Strenge genügen soll, mit den grössten Schwierigkeiten verbunden ist. Eines der merkwürdigsten Resultate dieser Art bietet sich dar, wenn man sämtliche Glieder der Reihe durch dieselbe übrigens ganz beliebige Zahl dividirt. Nimmt man die Primzahlen aus, die im Divisor aufgehen und mithin unter den ersten Gliedern der Reihe vorkommen, so werden alle übrigen einen Rest lassen, welcher relative Primzahl zum Divisor ist, und das Resultat, welches sich bei fortgesetzter Division herausstellt, besteht darin, dass jeder Rest der genannten Art unaufhörlich wiederkehrt, und zwar so, dass das Verhältniss der Zahlen, welche für irgend zwei solche Reste bezeichnen, wie oft sie bis zu einem gewissen Gliede erschienen sind, bei immer weiter fortgesetzter Division die Einheit zur Grenze hat. Abstrahirt man von der zunehmenden Gleichmässigkeit des Vorkommens der einzelnen Reste und beschränkt das Beobachtungsergebniss auf die nie aufhörende Wiederkehr eines jeden derselben, so lässt sich dasselbe in dem Satze aussprechen: „dass jede unbegrenzte arithmetische Reihe, deren erstes Glied und Differenz keinen gemeinschaftlichen Factor haben, unendlich viele Primzahlen enthält.“

Für diesen einfachen Satz existirte bis jetzt kein genügender Beweis, wie sehr auch ein solcher wegen der zahlreichen Anwendungen zu wünschen war, welche von dem Satze gemacht werden können. Der einzige Mathematiker, welcher die Begründung dieses Theorems versucht hat, ist, so viel ich weiss, LEGENDRE¹⁾, für den diese Untersuchung ausser dem Reiz, welcher in der Schwierigkeit des Gegenstandes liegt, noch ein ganz besonderes Interesse durch den Umstand haben musste, dass er die erwähnte Eigenschaft der arithmetischen Progression bei früheren Arbeiten als Lemma benutzt hatte. LEGENDRE macht den zu beweisenden Satz von der Aufgabe abhängig, die grösste Anzahl auf einander folgender Glieder einer arithmetischen Reihe zu finden, welche durch gegebene Primzahlen theilbar sein können, löst aber diese Aufgabe nur durch Induction. Versucht man, die auf diese Weise von ihm gefundene, durch die Einfachheit der Form des Resultates höchst merkwürdige Auflösung der Maximumsaufgabe zu beweisen, so stösst man auf grosse Schwierigkeiten, deren Ueberwindung mir nicht hat gelingen wollen. Erst nachdem ich den von LEGENDRE eingeschlagenen Weg ganz verlassen hatte, bin ich auf einen völlig strengen Beweis des Theorems über die arithmetische Progression gekommen. Der von mir gefundene Beweis, welchen ich der Akademie in dieser Abhandlung vorzulegen die Ehre habe, ist nicht rein arithmetisch, sondern beruht zum Theil auf der Betrachtung stetig veränderlicher Grössen. Bei der Neuheit der dabei zur Anwendung kommenden Principien hat es mir zweckmässig geschienen, dem Beweise des Theorems in seiner ganzen Allgemeinheit die Behandlung des besonderen Falles voranzuschicken, in welchem die Differenz der Progression eine ungerade Primzahl ist.

§. 1.

Es sei p eine ungerade Primzahl und c eine primitive Wurzel derselben, so dass also die Reste der Potenzen:

$$c^0, c^1, c^2, \dots, c^{p-2}$$

bei der Division durch p , wenn man von ihrer Ordnung absieht, mit den Zahlen:

$$1, 2, 3, \dots, p-1$$

zusammenfallen. Ist n eine nicht durch p theilbare Zahl, so werden wir mit GAUSS den Exponenten $\gamma < p-1$, welcher der Congruenz $c^\gamma \equiv n \pmod{p}$

¹⁾ Theorie des Nombres, 4^{ème} Partie, §. IX.

genügt, den Index von n nennen und, falls es nöthig sein sollte, mit γ_n bezeichnen. Die Wahl der primitiven Wurzel ω ist gleichgültig, nur soll angenommen werden, dass man die einmal gewählte nicht ändere. In Bezug auf die eben definirten Indices gilt der leicht zu beweisende Satz, dass der Index eines Productes der Summe der Indices der Factoren, um das darin enthaltene Vielfache von $p-1$ vermindert, gleich ist. Ferner bemerke man, dass immer $\gamma_1 = 0$, $\gamma_{p-1} = \frac{1}{2}(p-1)$, so wie dass γ_n gerade oder ungerade sein wird, je nachdem n Quadratrest oder Nichtquadratrest von p ist, oder mit Anwendung des LEGENDRE'schen Zeichens, je nachdem:

$$\left(\frac{n}{p}\right) = +1 \quad \text{oder} \quad \left(\frac{n}{p}\right) = -1$$

ist.

Es sei nun q irgend eine von p verschiedene Primzahl (2 nicht ausgeschlossen), und s eine positive die Einheit übersteigende Grösse. Man bezeichne ferner mit ω irgend eine Wurzel der Gleichung:

$$(1) \quad \omega^{p-1} - 1 = 0$$

und bilde die geometrische Reihe:

$$(2) \quad \frac{1}{1 - \omega^\gamma \frac{1}{q^s}} = 1 + \omega^\gamma \frac{1}{q^s} + \omega^{2\gamma} \frac{1}{q^{2s}} + \omega^{3\gamma} \frac{1}{q^{3s}} + \dots,$$

in welcher γ den Index von q bedeutet. Denkt man sich für q alle von p verschiedenen Primzahlen gesetzt und multiplicirt die so entstehenden Gleichungen in einander, so erhält man auf der zweiten Seite eine Reihe, deren Gesetz leicht zu erkennen ist. Ist nämlich n irgend eine nicht durch p theilbare ganze Zahl, und setzt man $n = q^m q'^m \dots$, wo q', q'', \dots verschiedene Primzahlen bezeichnen, so wird das allgemeine Glied die Form haben:

$$\omega^{m'\gamma_q + m''\gamma_{q''} + \dots} \frac{1}{n^s}.$$

Nun ist aber:

$$m'\gamma_q + m''\gamma_{q''} + \dots \equiv \gamma_n \pmod{p-1},$$

und folglich wegen (1):

$$\omega^{m'\gamma_q + m''\gamma_{q''} + \dots} = \omega^{\gamma_n}.$$

Man hat daher die Gleichung:

$$(3) \quad \prod \frac{1}{1 - \omega^\gamma \frac{1}{q^s}} = \sum \omega^\gamma \frac{1}{n^s} = L,$$

wo sich das Multiplicationszeichen auf die ganze Reihe der Primzahlen, mit alleiniger Ausnahme von p , erstreckt, während die Summation sich auf alle ganzen Zahlen von 1 bis ∞ bezieht, welche nicht durch p theilbar sind. Der Buchstabe γ bedeutet auf der ersten Seite γ_1 , auf der zweiten dagegen γ_n .

Die eben gefundene Gleichung repräsentirt $p-1$ verschiedene Gleichungen, welche man erhält, wenn man für ω seine $p-1$ Werthe setzt. Bekanntlich lassen sich diese $p-1$ verschiedenen Werthe durch die Potenzen von einem derselben Ω darstellen, wenn dieser gehörig gewählt wird, und sind dann:

$$\Omega^0, \Omega^1, \Omega^2, \dots, \Omega^{p-2}.$$

Wir werden, dieser Darstellung entsprechend, die verschiedenen Werthe L der Reihe oder des Productes mit:

$$(4) \quad L_0, L_1, L_2, \dots, L_{p-2}$$

bezeichnen, wobei es einleuchtet, dass L_0 und $L_{\frac{1}{2}(p-1)}$ eine von der Wahl des Werthes Ω unabhängige Bedeutung haben und sich resp. auf $\omega = 1$, $\omega = -1$ beziehen.

Ehe wir weiter gehen, ist es nöthig, den Grund der oben gemachten Voraussetzung anzugeben, nach welcher $s > 1$ sein sollte. Man überzeugt sich von der Nothwendigkeit dieser Beschränkung, wenn man auf den wesentlichen Unterschied Rücksicht nimmt, welcher zwischen zwei Arten von unendlichen Reihen stattfindet. Betrachtet man statt jedes Gliedes seinen Zahlenwerth oder, wenn es imaginär ist, seinen Modul, so können zwei Fälle eintreten. Es lässt sich nämlich entweder eine endliche Grösse angeben, welche die Summe von irgend welchen und noch so vielen dieser Zahlenwerthe oder Moduln stets übertrifft, oder diese Bedingung wird von keiner noch so grossen aber endlichen Zahl erfüllt. Im ersteren Falle ist die Reihe immer convergirend und hat eine völlig bestimmte Summe, welche von der Anordnung der Glieder ganz unabhängig ist, sei es nun, dass diese nur nach einer Dimension, sei es, dass sie nach zwei oder mehr Dimensionen fortschreiten, und eine sogenannte Doppel- oder vielfache Reihe bilden. Im zweiten der eben unterschiedenen Fälle kann zwar die Reihe auch noch convergiren, aber diese Eigenschaft, so wie die Summe der Reihe, werden wesentlich durch die Art der Aufeinanderfolge der Glieder bedingt sein. Findet die Convergenz für eine gewisse Ordnung statt, so kann sie durch Aenderung dieser Ordnung aufhören, oder es kann, wenn dies nicht der Fall ist, die Summe der Reihe eine ganz andere werden. So ist z. B. von

den beiden aus denselben Gliedern gebildeten Reihen:

$$1 - \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} - \frac{1}{\sqrt{4}} + \frac{1}{\sqrt{5}} - \frac{1}{\sqrt{6}} + \dots$$

$$1 + \frac{1}{\sqrt{3}} - \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{5}} + \frac{1}{\sqrt{7}} - \frac{1}{\sqrt{4}} + \dots$$

nur die erste convergirend, während die folgenden:

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \dots,$$

$$1 + \frac{1}{3} - \frac{1}{2} + \frac{1}{5} + \frac{1}{7} - \frac{1}{4} + \dots$$

zwar beide convergiren, aber keinesweges dieselbe Summe haben.

Was nun unsere unendliche Reihe L betrifft, so gehört diese, wie leicht zu sehen ist, nur dann in die erste der beiden eben unterschiedenen Classen, wenn man $s > 1$ annimmt, so dass also unter dieser Voraussetzung, wenn man $L = \lambda + \mu \sqrt{-1}$ setzt, λ und μ völlig bestimmte endliche Werthe sind. Bezeichnet man nun mit:

$$f_m + g_m \sqrt{-1}$$

das Product der m ersten Factoren der Form:

$$\frac{1}{1 - \omega^q}$$

diese Factoren in einer beliebigen Ordnung gedacht, so wird man immer m so gross nehmen können, dass sich unter diesen m ersten Factoren alle diejenigen befinden, in denen $q < h$ ist, wo h irgend eine ganze Zahl bezeichnet. Sobald m diesen Grad von Grösse erreicht hat, wird offenbar jede der beiden Differenzen $f_m - \lambda$, $g_m - \mu$, abgesehen vom Zeichen, immerfort kleiner bleiben als:

$$\frac{1}{h^s} + \frac{1}{(h+1)^s} + \dots,$$

wie weit man sich auch m noch ferner wachsend denke. Unter der Annahme $s > 1$ kann aber:

$$\frac{1}{h^s} + \frac{1}{(h+1)^s} + \dots$$

für ein gehörig grosses h beliebig klein werden. Es ist somit bewiesen, dass das unendliche Product in (3) einen von der Ordnung seiner Factoren unabhängigen, der Reihe L gleichen Werth hat. Ist hingegen $s = 1$ oder $s < 1$,

so ist dieser Beweis nicht mehr anwendbar, und in der That hat das unendliche Product in diesem Falle im Allgemeinen und unabhängig von der Ordnung der Factoren keinen bestimmten Werth mehr. Liesse sich bei einer gegebenen Art der Aufeinanderfolge der Factoren die Existenz eines Grenzwertes für die ins Unendliche fortgesetzte Multiplication nachweisen, so würde zwar die Gleichung (3), gehörig verstanden, noch stattfinden aber zur Feststellung dieses Werthes keinen wesentlichen Nutzen mehr gewähren. Man müsste nämlich, wenn q' , q'' , q''' , ... die der angenommenen Ordnung entsprechenden Werthe von q sind, die Reihe L als eine so zu ordnende vielfache Reihe betrachten, dass man zuerst diejenigen Glieder zu nehmen hätte, in denen n nur den Primfactor q' enthält, dann diejenigen der übrigen, in denen n keine anderen Primfactoren als q' , q'' enthält, u. s. w. Durch die Nothwendigkeit, den Gliedern diese Ordnung zu geben, würde die Summation der Reihe eben so schwierig, als es die Untersuchung des Productes selbst ist, vor welchem die Reihe nur dann hinsichtlich der Einfachheit etwas voraus hat, wenn die Ordnung ihrer Glieder willkürlich ist, oder sich wenigstens nicht nach den Primfactoren in n richtet.

§. 2.

Setzt man $s = 1 + \varrho$, so bleibt die Gleichung (3) gültig, wie klein man auch die positive Grösse ϱ annehme. Wir wollen nun untersuchen, in welcher Art sich die darin enthaltene Reihe L ändert, wenn man ϱ unendlich klein werden lässt. Das Verhalten der Reihe ist in dieser Beziehung ein ganz verschiedenes, je nachdem ω der positiven Einheit gleich ist oder irgend einen anderen Werth hat. Um mit dem ersten Falle oder mit der Untersuchung von L_0 zu beginnen, betrachten wir die Summe:

$$S = \frac{1}{k^{1+\varrho}} + \frac{1}{(k+1)^{1+\varrho}} + \frac{1}{(k+2)^{1+\varrho}} + \dots$$

in welcher k eine positive Constante bezeichnet. Schreibt man in der bekannten Formel:

$$\int_0^1 x^{k-1} \log^{\varrho} \left(\frac{1}{x} \right) dx = \frac{\Gamma(1+\varrho)}{k^{1+\varrho}}$$

für k der Reihe nach k , $k+1$, $k+2$, ... und addirt, so kommt:

$$S = \frac{1}{\Gamma(1+\varrho)} \int_0^1 \log^{\varrho} \left(\frac{1}{x} \right) \frac{x^{k-1}}{1-x} dx.$$

Addirt man $\frac{1}{q}$ und subtrahirt zugleich:

$$\frac{1}{q} = \frac{\Gamma(\varrho)}{\Gamma(1+\varrho)} = \frac{1}{\Gamma(1+\varrho)} \int_0^1 \log^{\varrho-1} \left(\frac{1}{x} \right) dx,$$

so geht diese Gleichung über in:

$$S = \frac{1}{q} + \frac{1}{\Gamma(1+\varrho)} \int_0^1 \left(\frac{x^{k-1}}{1-x} - \frac{1}{\log \left(\frac{1}{x} \right)} \right) \log^{\varrho} \left(\frac{1}{x} \right) dx,$$

wo das zweite Glied für ein unendlich kleines q sich der endlichen Grenze:

$$\int_0^1 \left(\frac{x^{k-1}}{1-x} - \frac{1}{\log \left(\frac{1}{x} \right)} \right) dx$$

nähert.

Betrachtet man statt der Reihe S die allgemeinere, welche zwei positive Constanten a, b enthält:

$$\frac{1}{b^{1+\varrho}} + \frac{1}{(b+a)^{1+\varrho}} + \frac{1}{(b+2a)^{1+\varrho}} + \dots,$$

so braucht man diese nur in die Form:

$$\frac{1}{a^{1+\varrho}} \left(\left(\frac{b}{a} \right)^{1+\varrho} + \left(\frac{b}{a} + 1 \right)^{1+\varrho} + \left(\frac{b}{a} + 2 \right)^{1+\varrho} + \dots \right)$$

zu bringen und mit S zu vergleichen, um sogleich zu sehen, dass sie einem Ausdrücke von folgender Form gleich ist:

$$\frac{1}{a} \cdot \frac{1}{q} + g(\varrho),$$

wo $g(\varrho)$ für ein unendlich klein werdendes q sich einer endlichen Grenze nähert.

Die zu untersuchende Reihe L_n besteht aus $p-1$ Partialreihen, wie:

$$\frac{1}{m^{1+\varrho}} + \frac{1}{(p+m)^{1+\varrho}} + \frac{1}{(2p+m)^{1+\varrho}} + \dots,$$

wo man successive:

$$m = 1, 2, \dots, p-1$$

zu setzen hat. Man hat mithin:

$$(5) \quad L_n = \frac{p-1}{p} \cdot \frac{1}{q} + g(\varrho),$$

wo wieder $g(\varrho)$ eine Function von q ist, die für ein unendlich kleines q einen

endlichen Werth annimmt, welchen man nach dem Vorigen leicht durch ein bestimmtes Integral ausdrücken könnte, was jedoch zu unserm Zwecke nicht erforderlich ist. Die Gleichung (5) zeigt, dass L_n für ein unendlich kleines q den Werth ∞ erhält, und zwar so, dass $L_n - \frac{p-1}{p} \cdot \frac{1}{q}$ endlich bleibt.

§. 3.

Nachdem wir gefunden haben, nach welchem Gesetze unsere Reihe, wenn darin $\omega = 1$ angenommen wird, für abnehmende der Einheit sich nähernde Werthe von s sich ändert, bleibt uns dieselbe Untersuchung auf die übrigen Wurzeln ω der Gleichung $\omega^{p-1} - 1 = 0$ auszudehnen. Obgleich die Summe der Reihe L , so lange $s > 1$, von der Ordnung der Glieder unabhängig ist, so wird es doch für diese Untersuchung vorthellhaft sein, sich die Glieder einander so folgend zu denken, dass die Werthe von n wachsend fortschreiten. Es ist nämlich unter dieser Voraussetzung:

$$\sum \omega^{\nu} \frac{1}{n^s}$$

eine Function von s , welche für alle positiven Werthe von s stetig und endlich bleibt, so dass also namentlich die Grenze, der sich der Werth der Reihe nähert, wenn man darin $s = 1 + q$ setzt und q unendlich klein werden lässt, und welche von der Ordnung der Glieder unabhängig ist, durch:

$$\sum \omega^{\nu} \frac{1}{n}$$

ausgedrückt ist, was bei einer andern Ordnung nicht nothwendig der Fall wäre, indem für eine solche $\sum \omega^{\nu} \frac{1}{n}$ von $\sum \omega^{\nu} \frac{1}{n^{1+q}}$ um eine endliche Grösse verschieden sein oder auch gar keinen Werth haben kann.

Um die eben ausgesprochene Behauptung zu beweisen, bezeichne man mit h irgend eine ganze positive Zahl und drücke die Summe der $h(p-1)$ ersten Glieder der Reihe:

$$\sum \omega^{\nu} \frac{1}{n^s}$$

mit Hilfe der schon oben gebrauchten für jedes positive s gültigen Formel:

$$\int_0^1 x^{p-1} \log^{s-1} \left(\frac{1}{x} \right) dx = \frac{\Gamma(s)}{n}$$

durch ein bestimmtes Integral aus. Man erhält so für diese Summe:

$$\frac{1}{\Gamma(s)} \int_0^1 \frac{x^{s-1} f(x)}{1-x^p} \log^s \left(\frac{1}{x}\right) dx = \frac{1}{\Gamma(s)} \int_0^1 \frac{x^{s-1} f(x)}{1-x^p} x^{hp} \log^s \left(\frac{1}{x}\right) dx,$$

wo man zur Abkürzung:

$$f(x) = \omega^{\gamma_1} x + \omega^{\gamma_2} x^2 + \dots + \omega^{\gamma_{p-1}} x^{p-1}$$

gesetzt hat. Ist nun, wie wir voraussetzen, ω nicht $= 1$, so ist das Polynom

$\frac{1}{x} f(x)$ durch $1-x$ theilbar, denn man hat:

$$f(1) = \omega^{\gamma_1} + \omega^{\gamma_2} + \dots + \omega^{\gamma_{p-1}} = 1 + \omega + \dots + \omega^{p-2} = 0.$$

Befreit man daher Zähler und Nenner des Bruches unter dem Integralzeichen von dem gemeinschaftlichen Factor $1-x$, so wird derselbe:

$$\frac{t+u}{1+x+x^2+\dots+x^{p-1}} - \frac{1}{1-x}$$

wo t und u Polynome mit reellen Coefficienten bedeuten. Bezeichnen T und U die grössten Zahlenwerthe von t und u zwischen $x=0$ und $x=1$, so sind offenbar der reelle und imaginäre Theil des zweiten Integrals:

$$\frac{1}{\Gamma(s)} \int_0^1 \frac{x^{s-1} f(x)}{1-x^p} x^{hp} \log^s \left(\frac{1}{x}\right) dx$$

respective kleiner als:

$$\frac{T}{\Gamma(s)} \int_0^1 x^{hp} \log^s \left(\frac{1}{x}\right) dx = \frac{T}{(hp+1)^s}.$$

$$\frac{U}{\Gamma(s)} \int_0^1 x^{hp} \log^s \left(\frac{1}{x}\right) dx = \frac{U}{(hp+1)^s},$$

und das Integral verschwindet demnach für $h = \infty$. Die Reihe:

$$\sum \omega^{\gamma} \frac{1}{n^s}$$

ist also, bei der angenommenen Ordnung ihrer Glieder, convergirend, und man hat für ihre Summe den Ausdruck:

$$\sum \omega^{\gamma} \frac{1}{n^s} = \frac{1}{\Gamma(s)} \int_0^1 \frac{x^{s-1} f(x)}{1-x^p} \log^s \left(\frac{1}{x}\right) dx.$$

Diese Function von s bleibt nicht nur selbst, so lange $s > 0$ ist, stetig und end-

lich, sondern dieselbe Eigenschaft kommt auch ihrem nach s genommenen Differentialquotienten zu. Es genügt, um sich davon zu überzeugen, nach s zu differenzieren und zu berücksichtigen, dass $\Gamma'(s)$, $\frac{d\Gamma'(s)}{ds}$, ebenfalls stetig und endlich sind, so wie dass $\Gamma'(s)$ nicht Null wird, so lange s positiv bleibt.

Setzen wir daher:

$$\frac{1}{\Gamma(s)} \int_0^1 \frac{1}{x} f(x) \log^{-1} \left(\frac{1}{x} \right) dx = \psi(s) + \chi(s) V - 1,$$

wo $\psi(s)$ und $\chi(s)$ reelle Functionen bedeuten, so haben wir nach einem bekannten Satze für ein positives q :

$$(6) \quad \psi(1+q) = \psi(1) + q\psi'(1+\delta q), \quad \chi(1+q) = \chi(1) + q\chi'(1+\varepsilon q),$$

wo zur Abkürzung:

$$\psi'(s) = \frac{d\psi(s)}{ds}, \quad \chi'(s) = \frac{d\chi(s)}{ds}$$

gesetzt ist und δ und ε positive von q abhängige Brüche bedeuten.

Es versteht sich übrigens von selbst, dass für $\omega = -1$:

$$\chi(s) = 0$$

ist, und dass, wenn man von einer imaginären Wurzel ω zu ihrer conjugirten $\frac{1}{\omega}$ übergeht, $\psi(s)$ denselben Werth behält, $\chi(s)$ aber den entgegengesetzten annimmt.

§. 4.

Wir haben jetzt nachzuweisen, dass die endliche Grenze, der sich:

$$\sum \omega^n \frac{1}{n^{1+q}}$$

unter der Voraussetzung; dass ω nicht die Wurzel 1 bedeutet, nähert, wenn man das positive q unendlich klein werden lässt, von Null verschieden ist. Diese Grenze ist nach dem vorigen Paragraphen:

$$\sum \omega^n \frac{1}{n}$$

und durch das Integral:

$$\sum \omega^n \frac{1}{n} = - \int_0^1 \frac{1}{x} \frac{f(x)}{x^q - 1} dx$$

gegeben, welches sich leicht durch Logarithmen und Kreisfunctionen ausdrücken lässt.

Irgend ein Linearfactor des Nenners x^p-1 ist:

$$x - e^{\frac{2m\pi}{p}} \sqrt[p]{1},$$

wo m aus der Reihe $0, 1, 2, \dots, p-1$ zu nehmen ist. Zerlegt man:

$$\frac{1}{x} f(x)$$

$$x^p - 1$$

in Partialbrüche, so wird nach den bekannten Formeln der Zähler des Bruches:

$$A_m$$

$$x - e^{\frac{2m\pi}{p}} \sqrt[p]{1}$$

durch den Ausdruck:

$$\frac{1}{x} f(x)$$

$$x^p - 1$$

gegeben, wo $x = e^{\frac{2m\pi}{p}} \sqrt[p]{1}$ zu setzen ist. Man hat also:

$$A_m = \frac{1}{p} f\left(e^{\frac{2m\pi}{p}} \sqrt[p]{1}\right).$$

Substituiert man diesen Werth und bemerkt, dass $A_0 = 0$ ist, so erhält man:

$$\sum \omega^y \frac{1}{n} = -\frac{1}{p} \sum f\left(e^{\frac{2m\pi}{p}} \sqrt[p]{1}\right) \int_0^1 \frac{dx}{x - e^{\frac{2m\pi}{p}} \sqrt[p]{1}},$$

wo sich die Summe auf der zweiten Seite von $m = 1$ bis $m = p-1$ erstreckt.

Die Function:

$$f\left(e^{\frac{2m\pi}{p}} \sqrt[p]{1}\right)$$

ist die bekannte in der Kreistheilung vorkommende und lässt sich leicht auf:

$$f\left(e^{\frac{2\pi}{p}} \sqrt[p]{1}\right)$$

zurückführen. Es ist nämlich:

$$f\left(e^{\frac{2m\pi}{p}} \sqrt[p]{1}\right) = \sum \omega^{yg} e^{\frac{2\pi}{p}} \sqrt[p]{1},$$

wo sich die Summe von $g = 1$ bis $g = p-1$ erstreckt. Setzt man statt gm den jedesmaligen Rest h nach dem Modul p , so sind $1, 2, \dots, p-1$ die ver-

schiedenen Werthe von h , und man hat, wegen $gm \equiv h \pmod{p}$:

$$\gamma_g \equiv \gamma_h - \gamma_m \pmod{p-1}.$$

Schreibt man also zugleich $\gamma_h - \gamma_m$ für γ_g , was wegen der Gleichung $\omega^{p-1} - 1 = 0$ erlaubt ist, so kommt:

$$f\left(\frac{e^{\frac{2m\pi}{p}} - 1}{e^{\frac{2\pi}{p}} - 1}\right) = \omega^{-\gamma_m} \sum \omega^{\gamma_h} \rho^{\frac{2\pi}{p}} \sqrt[p]{-1} = \omega^{-\gamma_m} f\left(\frac{e^{\frac{2\pi}{p}} - 1}{e^{\frac{2\pi}{p}} - 1}\right).$$

Die obige Gleichung wird so:

$$\sum \omega^{\gamma} \frac{1}{n} = -\frac{1}{p} f\left(\frac{e^{\frac{2\pi}{p}} - 1}{e^{\frac{2\pi}{p}} - 1}\right) \sum \omega^{-\gamma_m} \int_0^1 \frac{dx}{x - e^{\frac{2m\pi}{p}} \sqrt[p]{-1}}.$$

Nun ist für einen positiven Bruch α :

$$\int_0^1 \frac{dx}{x - e^{2\alpha\pi} \sqrt[p]{-1}} = \log(2 \sin \alpha\pi) + \frac{\pi}{2} (1 - 2\alpha) \sqrt[p]{-1},$$

folglich:

$$\sum \omega^{\gamma} \frac{1}{n} = -\frac{1}{p} f\left(\frac{e^{\frac{2\pi}{p}} - 1}{e^{\frac{2\pi}{p}} - 1}\right) \sum \omega^{-\gamma_m} \left(\log\left(2 \sin \frac{m\pi}{p}\right) + \frac{\pi}{2} \left(1 - \frac{2m}{p}\right) \sqrt[p]{-1} \right).$$

Obgleich dieser Ausdruck für $\sum \omega^{\gamma} \frac{1}{n}$ sehr einfach ist, so kann man doch im Allgemeinen nicht daraus schliessen, dass $\sum \omega^{\gamma} \frac{1}{n}$ einen von Null verschiedenen Werth hat. Es fehlt noch an gehörigen Principien zur Feststellung der Bedingungen, unter denen transcendente Verbindungen, welche unbestimmte ganze Zahlen enthalten, verschwinden können. Die verlangte Nachweisung gelingt jedoch für den besonderen Fall, wo $\omega = -1$ ist. Für die imaginären Werthe von ω werden wir im folgenden Paragraphen ein anderes Verfahren angeben, welches aber auf den genannten besonderen Fall nicht anwendbar ist.

Unter der Voraussetzung, dass $\omega = -1$ ist, erhält man, mit Berücksichtigung, dass γ_m gerade oder ungerade ist, je nachdem:

$$\left(\frac{m}{p}\right) = +1 \quad \text{oder} \quad = -1,$$

und dass folglich:

$$(-1)^{-\gamma_m} = \left(\frac{m}{p}\right)$$

ist, so wie dass:

$$(-1)^{\gamma_n} = \left(\frac{n}{p}\right),$$

als Grenze von $L_{\frac{1}{\rho}(\rho-1)}$ für ein unendlich klein werdendes ρ :

$$\Sigma\left(\frac{n}{\rho}\right) \frac{1}{n} = -\frac{1}{\rho} f\left(\frac{2\pi}{\rho^2} \rho^{-1}\right) \Sigma\left(\frac{m}{\rho}\right) \left(\log\left(2 \sin \frac{m\pi}{\rho}\right) + \frac{\pi}{2} \left(1 - \frac{2m}{\rho}\right) \rho^{-1}\right),$$

oder einfacher, da $\Sigma\left(\frac{m}{\rho}\right) = 0$ ist, wenn von $m = 1$ bis $m = \rho - 1$ summiert wird:

$$\Sigma\left(\frac{n}{\rho}\right) \frac{1}{n} = -\frac{1}{\rho} f\left(\frac{2\pi}{\rho^2} \rho^{-1}\right) \Sigma\left(\frac{m}{\rho}\right) \left(\log\left(2 \sin \frac{m\pi}{\rho}\right) - \frac{\pi}{\rho} m \rho^{-1}\right).$$

Es sind jetzt zwei Fälle zu unterscheiden, je nachdem die Primzahl ρ die Form $4\mu + 3$ oder $4\mu + 1$ hat. Im ersteren Falle ist für zwei Werthe, wie m und $\rho - m$, die sich zu ρ ergänzen:

$$\left(\frac{m}{\rho}\right) = -\left(\frac{\rho-m}{\rho}\right) \quad \text{und} \quad \sin \frac{m\pi}{\rho} = \sin \frac{(\rho-m)\pi}{\rho}.$$

Mithin verschwindet der reelle Theil der Summe, und man erhält, wenn man mit a die Werthe von m bezeichnet, für welche $\left(\frac{m}{\rho}\right) = 1$, und mit b diejenigen, für welche $\left(\frac{m}{\rho}\right) = -1$, oder mit anderen Worten, wenn a und b die Quadratreste und Nichtquadratreste von ρ bedeuten, welche kleiner als ρ sind:

$$\Sigma\left(\frac{n}{\rho}\right) \frac{1}{n} = \frac{\pi}{\rho^2} f\left(\frac{2\pi}{\rho^2} \rho^{-1}\right) (\Sigma a - \Sigma b) \rho^{-1}.$$

Ist $\rho = 4\mu + 1$, so verschwindet der imaginäre Theil der Summe, weil alsdann $\left(\frac{m}{\rho}\right) = \left(\frac{\rho-m}{\rho}\right)$, und man erhält:

$$\Sigma\left(\frac{n}{\rho}\right) \frac{1}{n} = \frac{1}{\rho} f\left(\frac{2\pi}{\rho^2} \rho^{-1}\right) \log \frac{H \sin \frac{b\pi}{\rho}}{H \sin \frac{a\pi}{\rho}},$$

wo sich die durch H angedeutete Multiplication auf alle a oder b erstreckt.

Bemerkt man jetzt, dass, unter der hier gemachten Annahme: $\omega = -1$, nach bekannten Formeln*)

$$f\left(\frac{2\pi}{\rho^2} \rho^{-1}\right) \text{ im ersteren Falle } \frac{1}{\rho} \rho^{-1}, \text{ im letzteren } \frac{1}{\rho}$$

ist, so kommt respective:

$$\Sigma\left(\frac{n}{\rho}\right) \frac{1}{n} = \frac{\pi}{\rho \sqrt{\rho}} (\Sigma b - \Sigma a), \quad \Sigma\left(\frac{n}{\rho}\right) \frac{1}{n} = \frac{1}{\sqrt{\rho}} \log \frac{H \sin \frac{b\pi}{\rho}}{H \sin \frac{a\pi}{\rho}}.$$

*) Comment. Gotting. rec. Vol. I oder die Abhandlungen unserer Akademie. Jahrg. 1835).

*) S. 9. Band II von Gauss' Werken oder S. 254 und S. 268 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

Für den Fall, wo $p = 4\mu + 3$ ist, sieht man sogleich, dass $\Sigma \binom{n}{p}^1$ von Null verschieden ist, indem $\Sigma a + \Sigma b = \frac{1}{2}p(p-1)$ ungerade ist und mithin nicht $\Sigma a = \Sigma b$ sein kann. Um dasselbe für $p = 4\mu + 1$ zu beweisen, nehme man die aus der Kreistheilung bekamten Gleichungen*) zu Hilfe:

$$2U(x - e^{\frac{2\pi}{p}})^{1-1} = Y - Z\sqrt{p}, \quad 2U(x - e^{\frac{2\pi}{p}})^{1-1} = Y + Z\sqrt{p},$$

wo Y und Z Polynome mit ganzen Coefficienten bedeuten. Setzt man in diesen Gleichungen und der daraus folgenden:

$$4 \frac{x^p - 1}{x - 1} = Y^2 - pZ^2$$

$x = 1$ und nennt g und h die ganzen Zahlen, welchen Y und Z gleich werden, so kommt, nach einigen leichten Reductionen:

$$2^{\frac{p+1}{2}} U \sin \frac{a\pi}{p} = g - h\sqrt{p}, \quad 2^{\frac{p+1}{2}} U \sin \frac{b\pi}{p} = g + h\sqrt{p}, \quad g^2 - ph^2 = 4p.$$

Aus der letzten Gleichung folgt, dass g durch p theilbar ist. Setzt man daher $g = pk$, und dividirt die beiden ersten durch einander, so erhält man:

$$\begin{aligned} U \sin \frac{b\pi}{p} \\ \frac{p}{p} &= \frac{k\sqrt{p+h}}{k\sqrt{p-h}}, \quad h^2 - pk^2 = -4. \\ U \sin \frac{a\pi}{p} \end{aligned}$$

Nach der zweiten dieser Gleichungen kann h nicht Null sein, folglich sind die beiden Seiten der ersten von der Einheit verschieden, woraus sogleich mit Berücksichtigung des oben erhaltenen Ausdruckes folgt, dass $\Sigma \binom{n}{p}^1$ nicht den Werth Null haben kann, w. z. b. w.

Man kann noch hinzufügen, dass die Summe $\Sigma \binom{n}{p}^1$, da sie als Grenzwert eines Products aus lauter positiven Factoren, nämlich als Grenzwert von:

$$U \frac{1}{1 - \left(\frac{q}{p}\right)^{\frac{1}{q^{1+p}}}}$$

für ein unendlich klein werdendes q auch nicht negativ sein kann, nothwendig positiv sein wird.

Aus dieser Bemerkung folgen unmittelbar zwei wichtige und auf anderem

*) Di-sq. arith. art. 357.

Wege wahrscheinlich sehr schwer zu beweisende Sätze, von denen der auf den Fall $p = 4\mu + 3$ bezügliche darin besteht, dass für eine Primzahl dieser Form immer $\Sigma b > \Sigma a$ ist. Wir wollen uns jedoch bei diesen Folgerungen unserer Methode hier nicht aufhalten, da wir bei einer anderen Untersuchung Gelegenheit finden werden, auf diesen Gegenstand zurückzukommen.

§. 5.

Um für L_m , wenn m weder 0 noch $\frac{1}{2}(p-1)$ ist, nachzuweisen, dass sein einem unendlich kleinen ϱ entsprechender Grenzwert von Null verschieden ist, nehme man den Logarithmus von:

$$H = \frac{1}{1 - \omega^\gamma} \frac{1}{q^{1+\varrho}}$$

und entwickle den Logarithmus jedes Factors mittelst der Formel:

$$-\log(1-x) = x + \frac{1}{2}x^2 + \frac{1}{3}x^3 + \dots$$

Man findet so:

$$\Sigma \omega^\gamma \frac{1}{q^{1+\varrho}} + \frac{1}{2} \Sigma \omega^{2\gamma} \frac{1}{(q^2)^{1+\varrho}} + \frac{1}{3} \Sigma \omega^{3\gamma} \frac{1}{(q^3)^{1+\varrho}} + \dots = \log L,$$

wo sich die Summationen auf q beziehen und γ den Index von q bedeutet.

Setzt man der Reihe nach für ω seine Werthe:

$$1, \Omega, \Omega^2, \dots, \Omega^{p-2},$$

addirt und berücksichtigt, dass die Summe:

$$1 + \Omega^{h\gamma} + \Omega^{2h\gamma} + \dots + \Omega^{(p-2)h\gamma}$$

immer verschwindet, ausser wenn $h\gamma$ durch $p-1$ theilbar ist, in diesem Falle aber den Werth $p-1$ hat, und dass die Bedingung $h\gamma \equiv 0 \pmod{p-1}$ gleichbedeutend mit $q^h \equiv 1 \pmod{p}$ ist, so erhält man:

$$(p-1) \left(\Sigma \frac{1}{q^{1+\varrho}} + \frac{1}{2} \Sigma \frac{1}{q^{2+2\varrho}} + \frac{1}{3} \Sigma \frac{1}{q^{3+3\varrho}} + \dots \right) = \log(L_0 L_1 \dots L_{p-2}),$$

wo sich die erste, zweite, ... Summation resp. auf die Werthe von q bezieht, deren erste, zweite, ... Potenzen in der Form $\mu p + 1$ enthalten sind. Da die erste Seite reell ist, so folgt, dass das Product unter dem Zeichen \log positiv ist, was auch sonst klar ist, und dass für den Logarithmus der arithmetische mit keiner Vieldeutigkeit behaftete Werth zu nehmen ist. Die Reihe auf der ersten Seite bleibt stets positiv, und wir werden nun zeigen, dass die zweite, in Widerspruch hiermit, für ein unendlich kleines ϱ den Werth $-\infty$ haben würde, wenn man die Grenze für L_m als verschwindend annehmen wollte. Die

zweite Seite lässt sich in die Form bringen:

$$\log L_0 + \log L_{\frac{1}{2}(p-1)} + \log L_1 L_{p-2} + \log L_2 L_{p-3} + \dots,$$

wo $\log L_n$ nach (5) dem Ausdrücke:

$$\log \left(\frac{p-1}{p} \cdot \frac{1}{q} + g(\varrho) \right)$$

oder:

$$\log \left(\frac{1}{q} \right) + \log \left(\frac{p-1}{p} + \varrho g(\varrho) \right)$$

gleich ist, dessen zweites Glied sich der endlichen Grenze $\log \left(\frac{p-1}{p} \right)$ nähert; ebenso bleibt $\log L_{\frac{1}{2}(p-1)}$ endlich, da der Grenzwert von $L_{\frac{1}{2}(p-1)}$ nach §. 4 von Null verschieden ist. Irgend einer der übrigen Logarithmen, wie $\log L_m L_{p-1-m}$, ist nach §. 3:

$$\log(\psi^2(1+\varrho) + \chi^2(1+\varrho)).$$

welcher Ausdruck, wenn L_m und also auch L_{p-1-m} die Null zur Grenze hätte, so dass gleichzeitig $\psi(1) = 0$, $\chi(1) = 0$ wäre, in:

$$\log(\varrho^2(\psi'^2(1+\delta\varrho) + \chi'^2(1+\varepsilon\varrho)))$$

oder:

$$-2 \log \left(\frac{1}{\varrho} \right) + \log(\psi'^2(1+\delta\varrho) + \chi'^2(1+\varepsilon\varrho))$$

übergehen würde. Vereinigt man das Glied $-2 \log \left(\frac{1}{\varrho} \right)$ mit dem ersten Gliede von $\log L_0$, so bleibt $-\log \left(\frac{1}{\varrho} \right)$, welcher Werth für ein unendlich kleines ϱ in $-\infty$ übergeht, und es ist klar, dass dieser unendlich grosse negative Werth nicht etwa durch:

$$\log(\psi'^2(1+\delta\varrho) + \chi'^2(1+\varepsilon\varrho))$$

aufgehoben werden kann, denn dieser Ausdruck bleibt entweder endlich oder wird selbst $-\infty$, wenn nämlich gleichzeitig $\psi'(1) = 0$, $\chi'(1) = 0$ wäre. Ebenso einleuchtend ist, dass, wenn man ausser L_m und L_{p-1-m} noch ein anderes oder mehrere andere Paare zusammengehöriger L als verschwindend betrachten wollte, der Widerspruch nur noch verstärkt würde. Es ist somit bewiesen, dass der einem unendlich klein werdenden ϱ entsprechende Grenzwert von L_m , für $m > 0$, endlich und von Null verschieden ist, so wie dass L_0 in demselben Falle ∞ wird, woraus sogleich folgt, dass die Reihe:

$$(7) \quad \sum \omega^r \frac{1}{q^{1+\varrho}} + \frac{1}{2} \sum \omega^{2r} \frac{1}{q^{2+2\varrho}} + \frac{1}{3} \sum \omega^{3r} \frac{1}{q^{3+3\varrho}} + \dots = \log L$$

sich immer, wenn nur nicht $\omega = 1$ ist, einer endlichen Grenze nähert, für $\omega = 1$ aber unendlich gross wird, wenn man ϱ unendlich klein werden lässt.

Wollte man diese endliche Grenze selbst haben, deren Kenntniss jedoch zu unserem Zwecke nicht erforderlich ist, so würde (wenn ω nicht -1 ist) ihre Bestimmung durch den Ausdruck $\log(\psi(1)+\chi(1)\sqrt{-1})$ mit einer Vieldeutigkeit behaftet sein, die man aber in jedem speciellen Falle, d. h. sobald p und ω numerisch gegeben sind, leicht heben kann. Setzt man die Reihe (7) gleich $u + v\sqrt{-1}$ und folglich:

$$u + v\sqrt{-1} = \log L = \log(\psi(1+\varrho) + \chi(1+\varrho)\sqrt{-1}),$$

so hat man:

$$u = \frac{1}{2} \log(\psi^2(1+\varrho) + \chi^2(1+\varrho)),$$

$$\cos v = \frac{\psi(1+\varrho)}{\sqrt{\psi^2(1+\varrho) + \chi^2(1+\varrho)}}, \quad \sin v = \frac{\chi(1+\varrho)}{\sqrt{\psi^2(1+\varrho) + \chi^2(1+\varrho)}}.$$

und folglich ist der Grenzwert von u ohne Vieldeutigkeit:

$$\frac{1}{2} \log(\psi^2(1) + \chi^2(1)).$$

Um den von v ebenso zu erhalten, bemerke man, dass die Reihe, wie klein auch ϱ sei, stetig mit dieser Grösse veränderlich ist, wie man leicht nachweisen kann, und dass mithin auch v eine stetige Function von ϱ sein muss. Nun wird sich, da nicht zugleich $\psi(1) = 0$, $\chi(1) = 0$ sein kann, aus den oben gegebenen Ausdrücken von $\psi(1+\varrho)$ und $\chi(1+\varrho)$ in Form bestimmter Integrale immer ein positiver endlicher Werth R von solcher Beschaffenheit ableiten lassen, dass wenigstens eine der Functionen $\psi(1+\varrho)$, $\chi(1+\varrho)$ für jedes ϱ , welches kleiner als R ist, dasselbe Zeichen behält. Es wird demnach $\cos v$ oder $\sin v$, sobald ϱ abnehmend kleiner als R geworden ist, sein Zeichen nicht mehr ändern und mithin der continuirlich veränderliche Bogen v nicht mehr um π zunehmen oder abnehmen können. Bestimmt man also den $\varrho = R$ entsprechenden endlichen Werth von v , den wir V nennen wollen, und den man durch numerische Rechnung aus der Reihe (7) selbst leicht finden kann, da diese für jeden endlichen Werth von ϱ in die erste der im §. 1 unterschiedenen Classen gehört und also eine völlig bestimmte Summe hat, so ist nun der Grenzwert v_0 von v durch die Gleichungen:

$$\cos v_0 = \frac{\psi(1)}{\sqrt{\psi^2(1) + \chi^2(1)}}, \quad \sin v_0 = \frac{\chi(1)}{\sqrt{\psi^2(1) + \chi^2(1)}},$$

mit der Bedingung verbunden, dass die Differenz $V - v_0$, abgesehen vom Zeichen, kleiner als π sein muss, vollständig bestimmt.

§. 6.

Wir sind jetzt im Stande zu beweisen, dass jede arithmetische Reihe, deren Differenz p ist, und deren erstes Glied nicht durch p theilbar ist, unendlich viele Primzahlen enthält, oder mit anderen Worten, dass es unendlich viele Primzahlen von der Form $\mu p + m$ giebt, wo μ eine unbestimmte ganze Zahl und m eine der Zahlen $1, 2, 3, \dots, p-1$ bedeutet. Denkt man sich die in der Gleichung (7) enthaltenen Gleichungen, so wie sie der Reihe nach den Wurzeln^{*)}:

$$1, \Omega, \Omega^2, \dots, \Omega^{p-2}$$

entsprechen, mit:

$$1, \Omega^{-\gamma m}, \Omega^{-2\gamma m}, \dots, \Omega^{-(p-2)\gamma m},$$

multiplirt und addirt, so erhält man auf der ersten Seite:

$$\begin{aligned} & \Sigma (1 + \Omega^{i-\gamma m} + \Omega^{2(i-\gamma m)} + \dots + \Omega^{(p-2)(i-\gamma m)}) \frac{1}{q^{1+e}} \\ & + \frac{1}{2} \Sigma (1 + \Omega^{2i-\gamma m} + \Omega^{3(2i-\gamma m)} + \dots + \Omega^{(p-2)(2i-\gamma m)}) \frac{1}{q^{2+2e}} \\ & + \frac{1}{3} \Sigma (1 + \Omega^{3i-\gamma m} + \Omega^{2(3i-\gamma m)} + \dots + \Omega^{p-2(3i-\gamma m)}) \frac{1}{q^{3+3e}} \\ & + \dots, \end{aligned}$$

wo sich die Summationen auf q beziehen und γ den Index von q bezeichnet. Nun ist aber:

$$1 + \Omega^{i-\gamma m} + \Omega^{2(i-\gamma m)} + \dots + \Omega^{(p-2)(i-\gamma m)} = 0,$$

ausser wenn $hi - \gamma m \equiv 0 \pmod{p-1}$ ist, in welchem Falle diese Summe gleich $p-1$ ist. Diese Congruenz ist aber gleichbedeutend mit: $q^i \equiv m \pmod{p}$. Man hat daher die Gleichung:

$$\begin{aligned} & \Sigma \frac{1}{q^{1+e}} + \frac{1}{2} \Sigma \frac{1}{q^{2+2e}} + \frac{1}{3} \Sigma \frac{1}{q^{3+3e}} + \dots \\ & = \frac{1}{p-1} (\log L_0 + \Omega^{-\gamma m} \log L_1 + \Omega^{-2\gamma m} \log L_2 + \dots + \Omega^{-(p-2)\gamma m} \log L_{p-2}), \end{aligned}$$

wo sich die erste Summation auf alle Primzahlen q der Form $\mu p + m$ erstreckt, die zweite auf alle Primzahlen q , deren Quadrate, die dritte auf alle Primzahlen q , deren Cuben, n. s. w. in derselben Form enthalten sind. Denkt man sich nun q unendlich klein werdend, so wird die zweite Seite durch das Glied $\log L_0$

^{*)} Vergl. S. 318. K.

unendlich gross. Es muss also auch die erste Seite unendlich werden. Auf dieser Seite bleibt aber die Summe aller Glieder, mit Ausschluss des ersten, endlich, da bekanntlich:

$$\frac{1}{2} \sum \frac{1}{q^2} + \frac{1}{3} \sum \frac{1}{q^3} + \dots$$

noch endlich ist, wenn man unter q nicht, wie hier, gewisse Primzahlen, sondern alle ganzen Zahlen, welche grösser als 1 sind, versteht. Folglich muss die Reihe:

$$\sum \frac{1}{q^{1+p}}$$

über jede positive Grenze hinaus wachsen: sie muss mithin unendlich viele Glieder enthalten, d. h. es giebt unendlich viele Primzahlen q der Form $ap + m$, w. z. b. w.

§. 7.

Um den im Vorhergehenden geführten Beweis auf eine arithmetische Reihe auszudehnen, deren Differenz irgend eine zusammengesetzte Zahl ist, sind einige Sätze aus der Theorie der Potenzreste erforderlich, die wir hier kurz zusammenstellen wollen, um uns in der Folge leichter darauf berufen zu können. Die Begründung dieser Resultate kann man in den *Disq. arith. sect. III.* nachsehen, wo dieser Gegenstand ausführlich behandelt ist.

I. Die Existenz von primitiven Wurzeln ist nicht auf ungerade Primzahlen p beschränkt, sondern findet auch noch für irgend eine Potenz p^π einer solchen statt. Ist c eine primitive Wurzel für den Modul p^π , so sind die nach diesem genommenen Reste der Potenzen:

$$c^0, c^1, c^2, \dots, c^{(p-1)p^{\pi-1}}$$

alle von einander verschieden und fallen mit der Reihe derjenigen Zahlen zusammen, welche kleiner als p^π und zu p^π relative Primzahlen sind. Hat man nun irgend eine nicht durch p theilbare Zahl n , so ist der Exponent $\gamma_n < (p-1)p^{\pi-1}$, welcher der Congruenz:

$$c^{\gamma_n} \equiv n \pmod{p^\pi}$$

genügt, völlig bestimmt und soll der Index von n heissen. Von solchen Indices gelten wieder die leicht zu beweisenden Sätze, dass der Index eines Productes der Summe der Indices der Factoren, um das grösste darin enthaltene Vielfache von $(p-1)p^{\pi-1}$ vermindert, gleich, so wie dass γ_n gerade oder ungerade ist, je nachdem $\binom{n}{p} = +1$ oder -1 ist.

II. Die Primzahl 2 verhält sich in der Theorie der primitiven Wurzeln wesentlich anders als die ungeraden Primzahlen, und es ist über diese Primzahl Folgendes zu bemerken, wenn wir die erste Potenz von 2, welche hier nicht in Betracht kommt, ausser Acht lassen.

1) Für den Modul 2^2 hat man die primitive Wurzel -1 . Bezeichnet man den Index für irgend eine ungerade Zahl n mit α_n , so dass also:

$$(-1)^{\alpha_n} \equiv n \pmod{4}.$$

so ist $\alpha_n = 0$ oder $\alpha_n = 1$, je nachdem n die Form $4\mu + 1$ oder $4\mu + 3$ hat, und man erhält den Index eines Productes, wenn man von der Summe der Indices der Factoren das grösste darin enthaltene Vielfache von 2 abzieht.

2) Hat der Modul die Form 2^k , wo $k \geq 3$ ist, so giebt es keine primitive Wurzel mehr, d. h. es existirt keine Zahl, für welche die Periode ihrer Potenzreste nach dem Divisor 2^k alle ungeraden Zahlen enthält, welche kleiner als 2^k sind. Man kann nur die Hälfte dieser Zahlen als solche Reste darstellen. Wählt man irgend eine Zahl der Form $8\mu + 5$ oder speciell 5 zur Basis, so sind die nach dem Modul 2^k genommenen Reste der Potenzen:

$$5^0, 5^1, 5^2, \dots, 5^{2^{k-2}-1}$$

alle von einander verschieden und fallen mit den Zahlen zusammen, welche die Form $4\mu + 1$ haben und kleiner als 2^k sind. Hat man daher eine Zahl n der Form $4\mu + 1$, so lässt sich immer der Congruenz:

$$5^{\beta_n} \equiv n \pmod{2^k}$$

durch einen und nur durch einen Exponenten oder Index β_n genügen, wenn dieser kleiner als 2^{k-2} sein soll. Hat n die Form $4\mu + 3$, so ist diese Congruenz unmöglich. Da aber unter dieser Voraussetzung $-n$ die Form $4\mu + 1$ hat, so wollen wir allgemein unter dem Index einer ungeraden Zahl n den völlig bestimmten Exponenten β_n verstehen, welcher kleiner als 2^{k-2} ist und der Congruenz:

$$5^{\beta_n} \equiv \pm n \pmod{2^k}$$

genügt, in welcher das obere oder das untere Zeichen zu nehmen ist, je nachdem n die Form $4\mu + 1$ oder $4\mu + 3$ hat. Wegen dieses doppelten Zeichens ist also der Rest von n nach dem Modul 2^k durch den Index β_n nicht mehr völlig bestimmt, indem demselben Index zwei Reste entsprechen, die sich zu 2^k ergänzen. Für die so definirten Indices gelten offenbar die Sätze, dass der Index eines Productes der Summe der Indices der Factoren, um das darin ent-

haltene grösste Vielfache von $2^{\lambda-2}$ vermindert, gleich ist, so wie dass β_n gerade oder ungerade sein wird, je nachdem n die Form $8\mu \pm 1$ oder die Form $8\mu \pm 5$ haben wird. Um die vorher erwähnte Zweideutigkeit zu heben, wird es genügen, neben dem Index β_n , welcher sich auf den Modul 2^λ und die Basis 5 bezieht, noch den Index α_n , welcher dem Modul 4 und der Basis -1 entspricht, zu betrachten, indem dann, je nachdem $\alpha_n = 0$ oder $\alpha_n = 1$ ist, das obere oder untere Zeichen in:

$$5^{\beta_n} \equiv \pm n \pmod{2^\lambda}$$

zu nehmen sein wird. Man kann auch, wenn man will, beide Indices in einer Formel vereinigen und:

$$(-1)^{\alpha_n} 5^{\beta_n} \equiv n \pmod{2^\lambda}$$

schreiben, durch welche Congruenz der Rest von n nach dem Modul 2^λ vollständig bestimmt ist.

III. Es sei nun:

$$k = 2^\lambda p^\alpha p'^{\alpha'} \dots,$$

wo, wie in II. 2. $\lambda \geq 3$ ist, und p, p', \dots von einander verschiedene ungerade Primzahlen bezeichnen. Hat man irgend eine durch keine der Primzahlen $2, p, p', \dots$ theilbare Zahl n , und kennt man die den Moduln:

$$4, 2^\lambda, p^\alpha, p'^{\alpha'}, \dots$$

und ihren primitiven Wurzeln:

$$-1, 5, c, c', \dots$$

entsprechenden Indices:

$$\alpha_n, \beta_n, \gamma_n, \gamma'_n, \dots$$

so hat man die Congruenzen:

$$\begin{aligned} (-1)^{\alpha_n} &\equiv n \pmod{4}, & 5^{\beta_n} &\equiv \pm n \pmod{2^\lambda}, \\ c^{\gamma_n} &\equiv n \pmod{p^\alpha}, & c'^{\gamma'_n} &\equiv n \pmod{p'^{\alpha'}}, \dots, \end{aligned}$$

durch deren Inbegriff der Rest von n , nach dem Divisor k genommen, vollständig bestimmt ist, wie aus bekannten Sätzen sogleich folgt, wenn man berücksichtigt, dass das doppelte Zeichen in der zweiten dieser Congruenzen durch die erste festgestellt wird. Wir werden die Indices $\alpha_n, \beta_n, \gamma_n, \gamma'_n, \dots$ oder $\alpha, \beta, \gamma, \gamma', \dots$ das System der Indices für die Zahl n nennen. Da die Indices:

$$\alpha, \beta, \gamma, \gamma', \dots$$

beziehungsweise:

$$2, 2^{\lambda-2}, (p-1)p^{\alpha-1}, (p'-1)p'^{\alpha'-1}, \dots$$

verschiedene Werthe erhalten können, so ist:

$$(8) \quad 2 \cdot 2^{p-2} (p-1) p^{p-1} \cdot (p'-1) p'^{p'-1} \dots = k \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{p'}\right) \dots = K$$

die Anzahl aller möglichen Systeme dieser Art, was mit dem bekannten Satze übereinstimmt, nach welchem K die Anzahl derjenigen Zahlen ausdrückt, welche kleiner als k und zu k relative Primzahlen sind.

§. 8.

Indem wir nun dazu übergehen, das Theorem über die arithmetische Progression in seiner ganzen Allgemeinheit zu beweisen, bemerken wir, dass man, ohne dieser Allgemeinheit zu schaden, die Differenz k der Progression als durch 8 theilbar und also in der Form des §. 7. III enthalten annehmen kann. Ist der Satz unter dieser Voraussetzung bewiesen, so wird er offenbar um so mehr gelten, wenn die Differenz ungerade oder nur durch 2 oder 4 theilbar ist. Es seien $\theta, q, \omega, \omega', \dots$ irgend welche Wurzeln der Gleichungen:

$$(9) \quad \theta^2 - 1 = 0, \quad q^{2^s - 2} - 1 = 0, \quad \omega^{p-1} p^{p-1} - 1 = 0, \quad \omega'^{(p'-1) p'^{p'-1}} - 1 = 0, \quad \dots$$

und q eine beliebige von 2, p, p', \dots verschiedene Primzahl. Bildet man nun die Gleichung:

$$1 - \frac{1}{1 - \theta^s q^\beta \omega^\gamma \omega'^{\gamma'} \dots} = 1 + \theta^s q^\beta \omega^\gamma \omega'^{\gamma'} \dots \frac{1}{q^s} + \theta^{2s} q^{2\beta} \omega^{2\gamma} \omega'^{2\gamma'} \dots \frac{1}{q^{2s}} + \dots,$$

in welcher $s \gg 1$ ist, und das System der Indices $\alpha, \beta, \gamma, \gamma', \dots$ sich auf q bezieht, und multiplicirt alle Gleichungen dieser Form, welche man erhält, wenn man für q alle von 2, p, p', \dots verschiedenen Primzahlen setzt, in einander, so kommt, mit Berücksichtigung der oben erwähnten Eigenschaften der Indices und der Gleichungen (9):

$$(10) \quad \prod \frac{1}{1 - \theta^s q^\beta \omega^\gamma \omega'^{\gamma'} \dots} = \sum \theta^s q^\beta \omega^\gamma \omega'^{\gamma'} \dots \frac{1}{n^s} = L,$$

wo sich das Multiplicationszeichen auf die ganze Reihe der Primzahlen, mit Ausschluss von 2, p, p', \dots , und das Summenzeichen auf alle positiven ganzen Zahlen, welche durch keine der Primzahlen 2, p, p', \dots theilbar sind, erstreckt. Das System der Indices $\alpha, \beta, \gamma, \gamma', \dots$ entspricht auf der ersten Seite der Zahl q , auf der zweiten Seite der Zahl n . Die allgemeine Gleichung (10), in

welcher die verschiedenen Wurzeln $\theta, \varphi, \omega, \omega', \dots$ auf irgend eine Weise mit einander combinirt werden können, enthält offenbar eine Anzahl K besonderer Gleichungen. Um die jeder dieser Verbindungen entsprechende Reihe L bequem zu bezeichnen, kann man sich die Wurzeln von jeder der Gleichungen (9) als Potenzen von einer derselben dargestellt denken. Sind $\Theta = -1, \Phi, \Omega, \Omega', \dots$ hierzu geeignete Wurzeln, so kann man setzen:

$$\theta = \Theta^a, \quad \varphi = \Phi^b, \quad \omega = \Omega^c, \quad \omega' = \Omega'^{c'}, \quad \dots,$$

wo:

$$a < 2, \quad b < 2^{\lambda-2}, \quad c < (p-1)p^{\pi-1}, \quad c' < (p'-1)p'^{\pi'-1}, \quad \dots,$$

und dieser Darstellung entsprechend, die Reihe L mit:

$$(11) \quad L_{a, b, c, c', \dots}$$

bezeichnen. Die Nothwendigkeit der Voraussetzung $s > 1$ in der Gleichung (10) beruht auf den schon im §. 1 entwickelten Gründen.

§. 9.

Die mit $L_{a, b, c, c', \dots}$ bezeichneten Reihen, deren Anzahl gleich K ist, lassen sich nach den verschiedenen Wurzelcombinationen $\theta, \varphi, \omega, \omega', \dots$ denen sie entsprechen, in folgende drei Classen theilen. Die erste Classe enthält nur eine Reihe, nämlich $L_{0, 0, 0, 0, \dots}$, d. h. diejenige, in welcher:

$$\theta = 1, \quad \varphi = 1, \quad \omega = 1, \quad \omega' = 1, \quad \dots$$

ist. Die zweite Classe soll alle übrigen Reihen umfassen, in welchen nur reelle Wurzeln der Gleichungen (9) vorkommen, so dass also zur Darstellung dieser Reihen die Zeichen in:

$$\theta = \pm 1, \quad \varphi = \pm 1, \quad \omega = \pm 1, \quad \omega' = \pm 1, \quad \dots$$

auf jede mögliche Weise combinirt werden müssen, wobei nur die eine der ersten Classe entsprechende Zeichenverbindung auszuschliessen ist. Die dritte Classe endlich wird alle Reihen L in sich begreifen, in denen wenigstens eine der Wurzeln $\varphi, \omega, \omega', \dots$ imaginär ist, und es leuchtet ein, dass die Reihen dieser Classe einander paarweise zugeordnet sind, da die beiden Wurzelcombinationen:

$$\theta, \varphi, \omega, \omega', \dots; \quad \frac{1}{\theta}, \frac{1}{\varphi}, \frac{1}{\omega}, \frac{1}{\omega'}, \dots$$

unter der eben ausgesprochenen Voraussetzung offenbar von einander verschieden

sind. Wir haben jetzt das Verhalten dieser Reihen zu untersuchen, wenn man darin $s = 1 + \varrho$ setzt und das positive ϱ unendlich klein werden lässt. Betrachten wir zunächst diejenige Reihe, welche die erste Classe constituirt, so ist klar, dass diese als die Summe von K Partialreihen angesehen werden kann, deren jede die Form hat:

$$\frac{1}{m^{1+\varrho}} + \frac{1}{(k+m)^{1+\varrho}} + \frac{1}{(2k+m)^{1+\varrho}} + \dots,$$

wo $m < k$ und zu k relative Primzahl ist. Mithin ist die Reihe dieser Classe nach §. 2 dem Ausdrucke:

$$(12) \quad \frac{K}{k} \cdot \frac{1}{\varrho} + \varrho(\varrho)$$

gleich, wo $\varrho(\varrho)$ für ein unendlich kleines ϱ endlich bleibt.

Was die Reihen der zweiten und dritten Classe betrifft, so findet man, wenn man sich darin die Glieder so geordnet denkt, dass die Werthe von n wachsend fortschreiten, und $s > 0$ setzt, für diese die Gleichung:

$$(13) \quad \Sigma \theta^\alpha g^\beta \omega^\gamma \omega'^{\gamma'} \dots \frac{1}{n^s} = \frac{1}{\Gamma(s)} \int_0^1 \frac{\Sigma \theta^\alpha g^\beta \omega^\gamma \omega'^{\gamma'} \dots x^{n-1}}{1-x^k} \log \left(\frac{1}{x} \right) dx,$$

wo sich das Zeichen Σ auf der zweiten Seite auf alle positiven ganzen Zahlen n erstreckt, welche kleiner als k und zu k relative Primzahlen sind, und $\alpha, \beta, \gamma, \gamma', \dots$ das System der Indices für n bedeutet. Man beweist leicht, dass die zweite Seite einen endlichen Werth hat, denn man darf hierzu nur bemerken, dass das Polynom $\Sigma \theta^\alpha g^\beta \omega^\gamma \omega'^{\gamma'} \dots x^{n-1}$ den Factor $1-x$ involvirt, was sogleich erhellt, wenn man $x = 1$ setzt, wodurch dieses Polynom in das Product:

$$(1+\theta)(1+g+\dots+g^{\lambda-2-1})(1+\omega+\dots+\omega^{(p-1)p^{\pi-1}-1})(1+\omega'+\dots+\omega'^{(p'-1)p'^{\pi'-1}-1})\dots$$

übergeht, von dessen Factoren wenigstens einer verschwindet, da die Wurzelcombination:

$$\theta = 1, \quad g = 1, \quad \omega = 1, \quad \omega' = 1, \quad \dots$$

als der ersten Classe entsprechend, ausgeschlossen ist. Ebenso leicht überzeugt man sich, dass die zweite Seite der Gleichung (13), so wie ihr nach s genommener Differentialquotient stetige Functionen von s sind. Es folgt hieraus sogleich, dass jede Reihe der zweiten und dritten Classe sich für ein unendlich klein werdendes ϱ einer endlichen, durch:

$$(14) \quad \Sigma \theta^\alpha g^\beta \omega^\gamma \omega'^{\gamma'} \dots \frac{1}{n} = \int_0^1 \frac{\Sigma \theta^\alpha g^\beta \omega^\gamma \omega'^{\gamma'} \dots x^{n-1}}{1-x^k} dx$$

ausgedrückten Grenze nähert. Es bleibt nun zu beweisen, dass diese Grenze immer von Null verschieden ist.

§. 10.

Die Grenze für ein L der zweiten oder dritten Classe lässt sich zwar leicht, wie in §. 4. durch Logarithmen und Kreisfunctionen ausdrücken, allein diese Darstellung derselben gewährt gar keinen Nutzen für die geforderte Nachweisung, selbst dann nicht, wenn L zur zweiten Classe gehört, obgleich dieser Fall sonst eine grosse Analogie mit dem in der letzten Hälfte des §. 4 betrachteten darbietet. Wir wollen für jetzt annehmen, die erwähnte Eigenschaft sei für jedes L der zweiten Classe bewiesen, und nun zeigen, wie derselben Forderung für ein L der dritten Classe genügt werden kann. Zu diesem Zwecke nehme man die Logarithmen von beiden Seiten der Gleichung (10) und entwickle: man erhält so:

$$\Sigma \theta^\alpha q^\beta \omega^\gamma \omega'^{\gamma'} \dots \frac{1}{q^{1+\alpha}} + \frac{1}{2} \Sigma \theta^{2\alpha} q^{2\beta} \omega^{2\gamma} \omega'^{2\gamma'} \dots \frac{1}{q^{2+2\alpha}} + \dots = \log L,$$

wo die Indices $\alpha, \beta, \gamma, \gamma', \dots$ zu q gehören, und auch das Zeichen Σ sich auf q bezieht. Stellt man die Wurzeln $\theta, q, \omega, \omega', \dots$ auf die im §. 8 angegebene Weise dar und setzt:

$$\theta = \Theta^a, \quad q = \Phi^b, \quad \omega = \Omega^c, \quad \omega' = \Omega'^{c'}, \quad \dots,$$

so wird das allgemeine Glied der ersten Seite:

$$\frac{1}{h} \Sigma \Theta^{haa} \Phi^{hb\beta} \Omega^{h\gamma c} \Omega'^{h\gamma' c'} \dots \frac{1}{q^{h+h\alpha}},$$

während nach (11) für die zweite Seite:

$$\log L_{a, b, c, c', \dots}$$

zu schreiben ist.

Es sei nun m irgend eine ganze Zahl kleiner als k , welche keinen gemeinschaftlichen Factor mit k hat. Multiplicirt man auf beiden Seiten mit:

$$\Theta^{-am^3} \Phi^{-\beta m^3} \Omega^{-\gamma m^3} \Omega'^{-\gamma' m^3} \dots$$

und schreibt zur Abkürzung auf der ersten Seite nur das allgemeine Glied, so kommt:

$$\begin{aligned} \dots + \frac{1}{h} \Sigma \Theta^{(ha-am^3)a} \Phi^{(hb-\beta m^3)b} \Omega^{(h\gamma-\gamma m^3)c} \Omega'^{(h\gamma'-\gamma' m^3)c'} \dots \frac{1}{q^{h+h\alpha}} + \dots \\ = \Theta^{-am^3} \Phi^{-\beta m^3} \Omega^{-\gamma m^3} \Omega'^{-\gamma' m^3} \dots \log L_{a, b, c, c', \dots} \end{aligned}$$

Summiert man jetzt, um alle Wurzelcombinationen zu umfassen, von:

$$a = 0, \quad b = 0, \quad c = 0, \quad c' = 0, \quad \dots$$

bis:

$$a = 1, \quad b = 2^{\lambda-2} - 1, \quad c = (p-1)p^{\pi-1} - 1, \quad c' = (p'-1)p'^{\pi'-1} - 1, \quad \dots,$$

so kommt auf der ersten Seite als allgemeines Glied:

$$\frac{1}{h} \Sigma W \frac{1}{q^{h+hq}}.$$

wo sich das Zeichen Σ auf die Primzahlen q erstreckt und W das Product der nach a. b. c. c'. . . resp. zwischen den angegebenen Grenzen zu nehmenden Summen:

$$\Sigma \Theta^{(ha-a_m)a}, \quad \Sigma \Phi^{(h\beta-\beta_m)b}, \quad \Sigma \Omega^{(h\gamma-\gamma_m)c}, \quad \Sigma \Omega'^{(h\gamma'-\gamma'_m)c'}, \quad \dots$$

bedeutet. Nun ersieht man leicht aus §. 7, dass die erste dieser Summen 2 oder 0 ist, je nachdem die Congruenz $ha - a_m \equiv 0 \pmod{2}$, oder was dasselbe ist, die Congruenz $q^h \equiv m \pmod{4}$ stattfindet oder nicht stattfindet, dass die zweite $2^{\lambda-2}$ oder 0 ist, je nachdem die Congruenz $h\beta - \beta_m \equiv 0 \pmod{2^{\lambda-2}}$, oder was dasselbe ist, die Congruenz $q^h \equiv \pm m \pmod{2^\lambda}$ stattfindet oder nicht stattfindet, dass die dritte $(p-1)p^{\pi-1}$ oder 0 ist, je nachdem die Congruenz $h\gamma - \gamma_m \equiv 0 \pmod{(p-1)p^{\pi-1}}$, oder was dasselbe ist, die Congruenz $q^h \equiv m \pmod{p^\pi}$ stattfindet oder nicht stattfindet, u. s. w. dass also W immer verschwindet, ausser wenn die Congruenz $q^h \equiv m$ nach jedem der Moduln $2^\lambda, p^\pi, p'^{\pi'}, \dots$ stattfindet, d. h. wenn $q^h \equiv m \pmod{k}$ ist, in welchem Falle $W = K$ wird. Unsere Gleichung wird daher:

$$(15) \quad \left\{ \begin{aligned} & \Sigma \frac{1}{q^{1+q}} + \frac{1}{2} \Sigma \frac{1}{q^{2+2q}} + \frac{1}{3} \Sigma \frac{1}{q^{3+3q}} + \dots \\ & = \frac{1}{K} \Sigma \Theta^{-a_m a} \Phi^{-\beta_m b} \Omega^{-\gamma_m c} \Omega'^{-\gamma'_m c'} \dots \log L_{a, b, c, c', \dots}, \end{aligned} \right.$$

wo sich die Summationen auf der ersten Seite resp. auf alle Primzahlen q beziehen, deren erste, zweite, dritte Potenzen in der Form $\mu k + m$ enthalten sind, während die Summation auf der zweiten Seite über a, b, c, c'. . . zwischen den schon angegebenen Grenzen zu erstrecken ist. Im Falle $m = 1$, wird $a_m = 0$, $\beta_m = 0$, $\gamma_m = 0$, $\gamma'_m = 0$, . . . und die zweite Seite reducirt sich auf:

$$\frac{1}{K} \Sigma \log L_{a, b, c, c', \dots}$$

Unter den Gliedern dieser Summe wird dasjenige, welches dem L der ersten Classe, $L_{0,0,0,0,\dots}$ entspricht, vermöge des mit (12) bezeichneten Ausdruckes, $\log \left(\frac{1}{e} \right)$ enthalten. Diejenigen Glieder, welche den verschiedenen L der zweiten

Classe entsprechen, werden, unter Voraussetzung der oben geforderten Nachweisung, für ein unendlich kleines ϱ endlich bleiben. Wäre nun der Grenzwert für irgend ein L der dritten Classe der Null gleich, so würde, wie in §. 5. die Betrachtung der Continuität des Ausdruckes (13) für den Logarithmus dieses L , mit dem des ihm zugeordneten L verbunden, das Glied:

$$-2\log\left(\frac{1}{\varrho}\right)$$

ergeben, aus dessen Vereinigung mit $\log\left(\frac{1}{\varrho}\right)$ in $\log L_{a, a, a, \dots}$ noch $-\log\left(\frac{1}{\varrho}\right)$ bliebe, welches für ein unendlich klein werdendes ϱ den Werth $-\infty$ annimmt, während die erste Seite aus lauter positiven Gliedern besteht. Kein L der dritten Classe kann also den Grenzwert Null haben, und es folgt daher (unter Vorbehalt des noch zu gebenden Beweises für die Reihen der zweiten Classe), dass:

$$\log L_{a, b, c, c', \dots}$$

sich für ein unendlich klein werdendes ϱ immer einer endlichen Grenze nähert, ausgenommen, wenn gleichzeitig $a = 0$, $b = 0$, $c = 0$, $c' = 0, \dots$ ist, in welchem Falle dieser Logarithmus einen unendlich grossen Werth erhält.

Wendet man dieses Resultat auf die allgemeine Gleichung (15) an, so sieht man sogleich, dass die zweite Seite derselben für ein unendlich kleines ϱ unendlich wird, und zwar durch das Glied $\frac{1}{k} \log L_{v, a, a, a, \dots}$, welches über jede Grenze hinaus wächst, während alle übrigen endlich bleiben. Es muss also auch die erste Seite jede endliche Grenze überschreiten, woraus wie in §. 6 folgt, dass die Reihe $\sum \frac{1}{q^{1+v}}$ unendlich viele Glieder enthält, oder mit anderen Worten, dass die Anzahl derjenigen Primzahlen q , welche die Form $ku + m$ haben, in welcher μ eine unbestimmte ganze Zahl und m eine gegebene Zahl bezeichnet, die keinen gemeinschaftlichen Factor mit k hat, unendlich ist, w. z. b. w.

§. 11.

Was nun die zur Vervollständigung des eben entwickelten Beweises noch erforderliche Nachweisung betrifft, so reducirt sich diese nach dem unter (14) gegebenen Ausdrucke für den Grenzwert eines L der zweiten oder dritten Classe darauf, dass man zeige, dass für irgend eine Wurzelcombination der Form:

$$\pm 1, \pm 1, \pm 1, \pm 1, \dots,$$

mit alleiniger Ausnahme der folgenden:

$$+1, +1, +1, +1, \dots,$$

die Summe:

$$(16) \quad \Sigma(\pm 1)^{\alpha}(\pm 1)^{\beta}(\pm 1)^{\gamma}(\pm 1)^{\gamma'} \dots \frac{1}{n},$$

worin $\alpha, \beta, \gamma, \gamma', \dots$ das System der Indices für n bedeutet, und für n alle positiven ganzen, durch keine der Primzahlen $2, p, p', p'', \dots$ theilbaren Zahlen, so wie sie ihrer Grösse nach auf einander folgen, zu setzen sind, einen von der Null verschiedenen Werth hat. In der Abhandlung, so wie sie der Akademie ursprünglich vorgelegt wurde, hatte ich diese Eigenschaft durch indirecte und ziemlich complicirte Betrachtungen bewiesen. Ich habe mich aber später überzeugt, dass man denselben Zweck auf einem andern Wege weit kürzer erreicht. Die Principien, von welchen wir hier ausgegangen sind, lassen sich auf mehrere andere Probleme anwenden, zwischen denen und dem hier behandelten Gegenstande man zunächst keinen Zusammenhang vermuthen sollte. Namentlich kann man mit Hilfe dieser Principien die sehr interessante Aufgabe lösen, die Anzahl der verschiedenen quadratischen Formen zu bestimmen, welche einer beliebigen positiven oder negativen Determinante entsprechen, und man findet, dass diese Anzahl (was jedoch nicht die Endform des Resultates dieser Untersuchung ist) als Product von zwei Factoren dargestellt werden kann, wovon der erste eine sehr einfache Function der Determinante ist, welche für jede Determinante einen endlichen Werth hat, während der andere Factor durch eine Reihe ausgedrückt ist, die mit der obigen (16) zusammenfällt. Aus diesem Resultat folgt dann unmittelbar, dass die Summe (16) nie Null sein kann, da sonst für die entsprechende Determinante die Anzahl der quadratischen Formen sich auf Null reduciren würde, während diese Anzahl wirklich immer ≥ 1 ist.

Aus diesem Grunde werde ich meinen früheren Beweis für die genannte Eigenschaft der Reihe (16) hier weglassen, und wegen dieses Punktes auf die erwähnten Untersuchungen über die Anzahl der quadratischen Formen verweisen*), welche nächstens erscheinen werden, und aus welchen der zur Vollständigkeit der gegenwärtigen Abhandlung erforderliche Satz, wie schon bemerkt worden, als ein blosses Corollar hervorgeht.

*) Eine vorläufige Notiz über diesen Gegenstand findet man im CRELLE'schen Journal Band XVIII, unter dem Titel: Sur l'usage des séries infinies dans la théorie des nombres.†)

†) S. 357 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

SUR LA MANIÈRE
DE RÉSOUDRE L'ÉQUATION $t^2 - pu^2 = 1$
AU MOYEN DES FONCTIONS CIRCULAIRES.

PAR

M. G. LEJEUNE DIRICHLET.

SUR LA MANIÈRE DE RÉSOUDRE L'ÉQUATION $t^2 - pu^2 = 1$ AU MOYEN DES FONCTIONS CIRCULAIRES.

Dans un Mémoire que j'ai lu à l'Académie des sciences de Berlin, et dont on trouve un extrait dans le compte rendu pour le mois de juillet dernier, je me suis proposé de prouver rigoureusement que toute progression arithmétique indéfinie dont le premier terme et la différence sont des entiers sans diviseur commun, renferme nécessairement une infinité de nombres premiers. Les recherches que j'ai eu à faire pour arriver à une démonstration complète de cette proposition qui peut être employée avec succès dans différentes questions relatives aux nombres, m'ont donné lieu de remarquer un rapport assez singulier entre deux théories qui ne présentaient jusqu'à présent aucun point de contact.

On sait que l'équation $t^2 - pu^2 = 1$, dans laquelle p désigne un entier positif non-carré, est toujours résoluble en nombres entiers, et que cette proposition fondamentale dans la théorie des équations indéterminées du second degré, a été déduite par LAGRANGE de la considération de la fraction continue périodique qui résulte du développement du radical \sqrt{p} . Il est remarquable que la résolution de l'équation précédente puisse aussi se rattacher à la théorie des équations binômes dont la science est redevable à M. GAUSS. Il résulte non seulement de cette théorie que l'équation $t^2 - pu^2 = 1$ est toujours résoluble, mais on peut même en déduire des formules générales qui expriment les inconnues t et u en fonctions circulaires.

Quoique cette manière de traiter l'équation dont il s'agit soit applicable à tous les cas, je me bornerai dans cette note à développer celui où p est un nombre premier, ce cas suffisant pour faire connaître l'esprit de la méthode. Il est sans doute inutile d'ajouter que le mode de solution que nous allons in-

diquer, est beaucoup moins propre au calcul numérique que celui qui dérive de l'emploi des fractions continues, cette nouvelle manière de résoudre l'équation $t^2 - pu^2 = 1$ devant être envisagée seulement sous le rapport théorique et comme un rapprochement entre deux branches de la science des nombres.

Soit p un nombre premier impair et considérons l'équation:

$$(1) \quad \frac{x^p - 1}{x - 1} = X = 0.$$

Les racines de cette équation sont données par l'expression $e^{m \frac{2\pi}{p} \sqrt{-1}}$, dans laquelle e et π ont la signification ordinaire et m désigne un entier compris dans la suite:

$$1, 2, 3, \dots, p-1.$$

Parmi ces entiers il y a $\frac{1}{2}(p-1)$ résidus et autant de non-résidus quadratiques de p , que nous désignerons respectivement en les prenant dans un ordre quelconque par:

$$a_1, a_2, \dots, a_{\frac{1}{2}(p-1)} \quad \text{et} \quad b_1, b_2, \dots, b_{\frac{1}{2}(p-1)}.$$

Cela posé, il résulte de la théorie de M. GAUSS* qu'on a ces deux équations:

$$(2) \quad \begin{cases} Y + Z\sqrt{\pm p} = 2 \left(x - e^{a_1 \frac{2\pi}{p} \sqrt{-1}} \right) \left(x - e^{a_2 \frac{2\pi}{p} \sqrt{-1}} \right) \dots \left(x - e^{a_{\frac{1}{2}(p-1)} \frac{2\pi}{p} \sqrt{-1}} \right), \\ Y - Z\sqrt{\pm p} = 2 \left(x - e^{b_1 \frac{2\pi}{p} \sqrt{-1}} \right) \left(x - e^{b_2 \frac{2\pi}{p} \sqrt{-1}} \right) \dots \left(x - e^{b_{\frac{1}{2}(p-1)} \frac{2\pi}{p} \sqrt{-1}} \right), \end{cases}$$

les signes supérieurs ou inférieurs ayant lieu suivant que p a la forme $4\mu + 1$ ou $4\mu + 3$, et Y, Z étant des polynômes en x dont les coefficients sont entiers.

Les équations précédentes étant multipliées entre elles donnent:

$$(3) \quad 4X = Y^2 \mp pZ^2.$$

Comme les nombres:

$$a_1, a_2, \dots, a_{\frac{1}{2}(p-1)},$$

abstraction faite de l'ordre, sont les restes qui proviennent des carrés:

$$1^2, 2^2, \dots, \left(\frac{1}{2}(p-1)\right)^2$$

lorsqu'on les divise par p , la première des équations (2) peut évidemment être remplacée par celle-ci:

$$(4) \quad Y + Z\sqrt{\pm p} = 2 \left(x - e^{1^2 \frac{2\pi}{p} \sqrt{-1}} \right) \left(x - e^{2^2 \frac{2\pi}{p} \sqrt{-1}} \right) \dots \left(x - e^{\left(\frac{p-1}{2}\right)^2 \frac{2\pi}{p} \sqrt{-1}} \right).$$

Distinguons actuellement les deux cas que p peut présenter, et supposons en premier lieu p de la forme $4\mu + 1$. Faisant $x = 1$ dans les équations (3) et (4) et désignant par g et h les valeurs entières de Y et Z correspondant à

* Disquisitiones arithmeticae. Art. 357.

cette supposition, il viendra :

$$(5) \quad g^2 - ph^2 = 4p, \\ g + h\sqrt{p} = 2 \left(1 - e^{i^2 \cdot \frac{2\pi}{p}\sqrt{-1}} \right) \left(1 - e^{2^2 \cdot \frac{2\pi}{p}\sqrt{-1}} \right) \dots \left(1 - e^{\left(\frac{p-1}{2}\right)^2 \frac{2\pi}{p}\sqrt{-1}} \right).$$

Comme on peut écrire :

$$1 - e^{s^2 \cdot \frac{2\pi}{p}\sqrt{-1}} = -2\sqrt{-1} \cdot \sin s^2 \frac{\pi}{p} \cdot e^{s^2 \cdot \frac{\pi}{p}\sqrt{-1}},$$

la dernière équation prendra la forme :

$$g + h\sqrt{p} = 2^{j(p+1)} (-1)^{\frac{j}{2}(p-1)} \sin 1^2 \frac{\pi}{p} \cdot \sin 2^2 \frac{\pi}{p} \dots \sin \left(\frac{1}{2}(p-1)\right)^2 \frac{\pi}{p} \cdot e^{[1^2+2^2+\dots+(\frac{p-1}{2})^2] \frac{\pi}{p}\sqrt{-1}}.$$

On a d'un autre côté :

$$1 + 2^2 + \dots + \left(\frac{1}{2}(p-1)\right)^2 = p \frac{p^2-1}{24},$$

où $\frac{p^2-1}{24}$ est évidemment un entier pair ou impair suivant que p a la forme $8\mu+1$ ou $8\mu+5$. Le facteur exponentiel est donc suivant ces deux cas $+1$ ou -1 et peut par conséquent être exprimé par $(-1)^{\frac{j}{2}(p-1)}$. Substituant cette expression dans l'équation précédente et se rappelant que $\frac{1}{2}(p-1)$ est pair, il viendra :

$$g + h\sqrt{p} = 2^{j(p+1)} \sin 1^2 \frac{\pi}{p} \cdot \sin 2^2 \frac{\pi}{p} \dots \sin \left(\frac{1}{2}(p-1)\right)^2 \frac{\pi}{p}.$$

Il résulte de l'équation (5) que l'entier g est divisible par p ; en mettant donc pk à la place de g , on aura :

$$(6) \quad h^2 - pk^2 = -4, \\ h + k\sqrt{p} = \frac{2^{j(p+1)}}{\sqrt{p}} \sin 1^2 \frac{\pi}{p} \cdot \sin 2^2 \frac{\pi}{p} \dots \sin \left(\frac{1}{2}(p-1)\right)^2 \frac{\pi}{p} = a.$$

On voit donc qu'il existe des entiers h et k tels que :

$$h^2 - pk^2 = -4,$$

et que ces entiers peuvent généralement être exprimés par les fonctions circulaires, car l'on conclut facilement des équations précédentes :

$$h = \frac{a}{2} - \frac{2}{a}, \quad k = \frac{1}{\sqrt{p}} \left(\frac{a}{2} + \frac{2}{a} \right).$$

Pour passer à l'équation :

$$t^2 - pu^2 = 1,$$

il faudra distinguer le cas où p a la forme $8\mu+1$ et celui où $p = 8\mu+5$.

Dans le premier de ces deux cas, h et k seront évidemment pairs l'un et l'autre et l'on aura :

$$\left(\frac{h}{2}\right)^2 - p\left(\frac{k}{2}\right)^2 = -1,$$

d'où l'on conclut :

$$\left(\frac{h}{2} + \frac{k}{2}\sqrt{p}\right)^2 = t + u\sqrt{p},$$

les parties rationnelles et les coefficients de \sqrt{p} étant égaux séparément.

Lorsque p est de la forme $8\mu + 5$, h et k seront impairs l'un et l'autre. En posant alors :

$$(h+k\sqrt{p})^3 = h' + k'\sqrt{p}$$

et par conséquent :

$$h' = h^3 + 3phk^2, \quad k' = 3h^2k + pk^3,$$

on aura l'équation :

$$h'^2 - pk'^2 = -4^3.$$

Il est facile de voir que les nombres h' et k' sont l'un et l'autre divisibles par 8. Il suffit, pour s'en assurer, de les mettre, en ayant égard à l'équation (6) sous cette autre forme :

$$h' = 4h(pk^2 - 1), \quad k' = 4k(h^2 + 1).$$

L'équation précédente deviendra donc :

$$\left(\frac{h'}{8}\right)^2 - p\left(\frac{k'}{8}\right)^2 = -1,$$

d'où l'on déduit la solution de l'équation $t^2 - pu^2 = 1$, en posant, comme plus haut :

$$\left(\frac{h'}{8} + \frac{k'}{8}\sqrt{p}\right)^2 = t + u\sqrt{p}.$$

Considérons en second lieu le cas où p est de la forme $4\mu + 3$. Dans ce cas, les coefficients des termes à égale distance des extrêmes $2x^{\frac{1}{2}(p-1)}$ et -2 du polynôme Y ont les mêmes valeurs numériques avec des signes opposés, de sorte qu'on peut mettre ce polynôme sous la forme :

$$Y = 2(x^m - 1) + ax(x^{m-2} - 1) + bx^2(x^{m-4} - 1) + \dots,$$

en posant pour abrégier $m = \frac{1}{2}(p - 1)$.

Et comme, en attribuant à l'indéterminée x la valeur particulière $\sqrt{-1}$, on a :

$$\begin{aligned} x^m - 1 &= -(1 + \sqrt{-1}), & x(x^{m-2} - 1) &= -(1 + \sqrt{-1}), \\ x^2(x^{m-4} - 1) &= 1 + \sqrt{-1}, & x^3(x^{m-6} - 1) &= 1 + \sqrt{-1}, \text{ etc.} \end{aligned}$$

on :

$$x^m - 1 = -(1 - \sqrt{-1}), \quad x(x^{m-2} - 1) = 1 - \sqrt{-1},$$

$$x^2(x^{m-4} - 1) = 1 - \sqrt{-1}, \quad x^3(x^{m-6} - 1) = -(1 - \sqrt{-1}), \text{ etc.}$$

suivant que m a la forme $4\mu + 3$ ou $4\mu + 1$, c'est-à-dire, suivant que p a la forme $8\mu + 7$ ou $8\mu + 3$, on voit que le polynôme Y deviendra selon ces deux cas :

$$g(1 + \sqrt{-1}) \quad \text{ou} \quad g(1 - \sqrt{-1}),$$

g désignant un entier réel. Quant à l'autre polynôme Z dont les coefficients également distants du commencement et de la fin sont égaux, on trouve d'une manière toute semblable qu'il se réduit, pour $x = \sqrt{-1}$, à la forme $h(1 - \sqrt{-1})$ ou à celle-ci : $h(1 + \sqrt{-1})$, suivant qu'on a $p = 8\mu + 7$ ou $p = 8\mu + 3$, h désignant pareillement un entier réel.

Il résulte de là et de ce que l'on a évidemment $X = \sqrt{-1}$ pour $x = \sqrt{-1}$, que l'équation :

$$4X = Y^2 + pZ^2$$

deviendra dans cette même supposition :

$$g^2(1 \pm \sqrt{-1})^2 + ph^2(1 \mp \sqrt{-1})^2 = 4\sqrt{-1}.$$

les signes supérieurs ou inférieurs ayant lieu suivant que p a la forme $8\mu + 7$ ou $8\mu + 3$.

L'équation précédente est équivalente à celle-ci :

$$(1) \quad g^2 - ph^2 = \pm 2,$$

qui est donc toujours résoluble et de laquelle on passe facilement à l'équation $t^2 - pu^2 = 1$ en posant :

$$(g + h\sqrt{p})^2 = 2t + 2u\sqrt{p},$$

où t et u seront des entiers, g et h étant évidemment impairs. Pour exprimer ensuite g et h par des fonctions circulaires, l'on posera $x = \sqrt{-1}$ dans l'équation (4) et l'on combinera le résultat de cette substitution avec l'équation (7).

On voit que la solution que l'on vient d'indiquer, n'est qu'un corollaire très simple du théorème dû à M. GAUSS et d'après lequel le polynôme $4X$ peut toujours être mis sous la forme $Y^2 \mp pZ^2$, p étant un nombre premier. Pour étendre la même solution au cas général où p est un nombre composé, il faut donner une plus grande étendue au théorème cité. Cette généralisation ne présente aucune difficulté et peut se déduire des principes sur lesquels re-

pose l'analyse de M. GAUSS. C'est pourquoi je me contenterai d'indiquer le résultat pour le cas d'un nombre composé de deux facteurs premiers.

Les lettres p et q désignant deux nombres premiers impairs différents, on trouve que la fonction entière :

$$(8) \quad 4 \frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)}$$

peut encore se mettre sous la forme :

$$Y^2 \mp pqZ^2,$$

Y et Z désignant toujours des polynômes, dont tous les coefficients sont des entiers, et le signe supérieur ou le signe inférieur ayant lieu suivant que le produit pq a la forme $4\mu + 1$ ou $4\mu + 3$. Cette décomposition résulte, comme dans le cas particulier d'un seul nombre premier, de la distribution en deux groupes des racines de l'équation que l'on obtient en égalant l'expression (8) à zéro.

Voici un exemple de cette décomposition. Faisant $p = 3$, $q = 11$, on aura :

$$4 \frac{(x^{33} - 1)(x - 1)}{(x^3 - 1)(x^{11} - 1)} = Y^2 - 33Z^2,$$

$$Y = 2x^{10} - x^9 + 8x^8 + 5x^7 + 2x^6 + 14x^5 + 2x^4 + 5x^3 + 8x^2 - x + 2,$$

$$Z = x^9 + x^7 + 2x^6 + 2x^4 + x^3 + x.$$

ÜBER
DIE BESTIMMUNG ASYMPTOTISCHER GESETZE
IN DER ZAHLENTHEORIE.

VON

G. LEJEUNE DIRICHLET.

Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1838, S. 13—15.

ÜBER DIE BESTIMMUNG ASYMPTOTISCHER GESETZE IN DER ZAHLENTHEORIE.

[Auszug aus einer in der Akademie der Wissenschaften
am 8. Februar 1838 gelesenen Abhandlung.]

Es ist eine bekannte analytische Erscheinung, dass Functionen, deren Form um so zusammengesetzter wird, je grösser die Werthe sind, welche die unabhängige Veränderliche erhält, in vielen Fällen ungeachtet dieser scheinbar unaufhörlich steigenden Complication mit stets wachsender Regelmässigkeit sich ändern, so dass es einen einfachen Ausdruck giebt, der sich einer solchen Function immer inniger anschliesst und ihren Gang ungefähr so bezeichnet, wie eine Curve den Lauf einer andern darstellt, deren Asymptote sie ist. Man kann, auf die Analogie mit der Geometrie gestützt, eine solche einfache leicht zu überschende Function das asymptotische Gesetz der complicirteren nennen, nur muss man das Wort „asymptotisch“ im allgemeineren Sinne nehmen und auf den Quotienten beider beziehen, welcher als der Einheit unaufhörlich sich nähernd anzusehen ist, während ihre Differenz nicht nothwendig ins Unendliche abnimmt.

Das älteste Beispiel eines solchen asymptotischen Gesetzes bietet der merkwürdige Ausdruck:

$$\frac{2^{2n}}{\sqrt{n\pi}}$$

dar, welchen STIRLING zur genäherten Bestimmung des mittleren Binomialcoefficienten einer sehr hohen geraden Potenz aus dem früher von WALLIS gefundenen unendlichen Product für π abgeleitet hat. Spätere Untersuchungen haben eine Menge ähnlicher Resultate ergeben, die besonders für die Wahrscheinlichkeitsrechnung sehr wichtig geworden sind.

Die Existenz asymptotischer Gesetze ist nicht auf analytische Functionen beschränkt, sondern kann auch noch stattfinden, wo ein analytischer Ausdruck ganz fehlt, wie dies gewöhnlich bei den Functionen der Fall ist, welche sich auf Eigenschaften der Zahlen beziehen. So hat namentlich LEGENDRE durch Induction eine sehr merkwürdige Formel gefunden, welche auf eine sehr genährte Weise die Anzahl der Primzahlen ausdrückt, die eine gegebene Grenze nicht übersteigen. Die *Disquisitiones arithmeticae* enthalten ebenfalls mehrere höchst interessante Ausdrücke ähnlicher Art, welche der Theorie der quadratischen Formen angehören und die mittlere Anzahl der Classen und Ordnungen solcher Formen in Function der Determinante darstellen. Für diese Ausdrücke ist aber bisher ebenso wenig als für die LEGENDRESche Formel ein Beweis bekannt geworden.

Die der Akademie vorgelegte Abhandlung hat den Zweck, mehrere Methoden zu entwickeln, welche bei Untersuchungen dieser Art in vielen Fällen mit Erfolg benutzt werden können, und deren Anwendung ausser verschiedenen andern Resultaten auch die LEGENDRESche Formel und einige der von GAUSS mitgetheilten ergibt. Wir müssen uns in diesem Auszuge darauf beschränken, von einer dieser Methoden ein Beispiel an einem Problem zu zeigen, welches bisher nicht behandelt worden ist und sich auf die Theorie der Theiler bezieht.

Bezeichnet b_n die Anzahl der Divisoren von n (1 und n selbst mitgerechnet), so ist b_n eine sehr unregelmässig fortschreitende Function von n , die, obgleich im Ganzen mit n über alle Grenzen hinaus wachsend, dennoch unendlich oft sehr kleine Werthe wie 2, 3, ... annimmt. Betrachtet man aber statt dieser Function ihren mittleren Werth, diesen Ausdruck in dem Sinne genommen, wie derselbe in den *Disq. arith.* pag. 515¹⁾ defint ist, so verschwindet die Unregelmässigkeit, und dieser mittlere Werth wird eines asymptotischen Gesetzes fähig.

Zur Bestimmung desselben betrachte man die unendliche Reihe:

$$b_1 q + b_2 q^2 + \dots + b_n q^n + \dots = f(q),$$

welche, wie schon LAMBERT bemerkt hat, auch in folgender Form dargestellt werden kann:

$$\frac{q}{1-q} + \frac{q^2}{1-q^2} + \dots + \frac{q^n}{1-q^n} + \dots = f(q).$$

¹⁾ Gauss' Werke, Band I, S. 363. K.

Die Summe dieser Reihe bleibt endlich, so lange ϱ ein echter Bruch ist, und wächst über jede Grenze hinaus, während sich ϱ (welches als positiv betrachtet wird) der Einheit nähert. Setzt man:

$$\varrho = e^{-\alpha}$$

und drückt die Reihe durch ein bestimmtes Integral aus, so findet man leicht, dass dieselbe für unendlich kleine positive Werthe von α durch den einfachen Ausdruck:

$$\frac{1}{\alpha} \log\left(\frac{1}{\alpha}\right) + \frac{C}{\alpha}$$

dargestellt wird, in welchem C die bekannte EULER'sche Constante bezeichnet, deren Werth:

$$0,5772156649, \dots$$

ist.*)

Man übersieht bald, dass zwischen dem vorhergehenden Ausdruck, der den Grad der Schnelligkeit des Wachsens der Function:

$$b_1 e^{-\alpha} + b_2 e^{-2\alpha} + \dots + b_n e^{-n\alpha} + \dots$$

ausspricht und als ihr asymptotisches Gesetz für abnehmende Werthe von α anzusehen ist, und dem mittleren Werthe des allgemeinen Coefficienten b_n ein notwendiger Zusammenhang stattfindet. Eine genauere auf die Eigenschaften der bekannten Integrale:

$$\Gamma(k) = \int_0^{\infty} e^{-x} x^{k-1} dx, \quad \Gamma'(k) = \int_0^{\infty} e^{-x} x^{k-1} \log x dx$$

gegründete Untersuchung ergibt dann für das asymptotische Gesetz von b_n den Ausdruck:

$$\log n + 2C.$$

Summirt man diesen von $n = 1$ bis $n = n$, so erhält man für das asymptotische Gesetz der Summe:

$$b_1 + b_2 + \dots + b_n$$

die Formel:

$$\left(n + \frac{1}{2}\right) \log n + n + 2Cn,$$

welche eine sehr grosse Annäherung gewährt.

*) Institutiones calculi differentialis, Caput VI, 143, p. 444.

Man erhält z. B. für $n = 100$:

$$b_1 + b_2 + \dots + b_n = 482$$

und:

$$(n + \frac{1}{2}) \log n + n + 2Cn = 478,2,$$

für $n = 200$:

$$b_1 + b_2 + \dots + b_n = 1098$$

und:

$$(n + \frac{1}{2}) \log n + n + 2Cn = 1093,2.$$

Wollte man statt der mittleren Anzahl die mittlere Summe der Divisoren von n bestimmen, so müsste man statt der LAMBERT'schen Reihe die folgende betrachten:

$$\frac{e}{(1-e)^2} + \frac{e^2}{(1-e^2)^2} + \dots + \frac{e^n}{(1-e^n)^2} + \dots$$

welche, wenn man sie nach Potenzen von e entwickelt, in ihrem allgemeinen Gliede:

$$c_n e^n$$

die Summe der Divisoren von n zum Coefficienten hat. Aehnliche Betrachtungen ergeben für den mittleren Werth dieses Coefficienten den asymptotischen Ausdruck:

$$\frac{1}{6} \pi^2 n - \frac{1}{2}.$$

SUR L'USAGE DES SÉRIES INFINIES
DANS LA THÉORIE DES NOMBRES.

PAR

M. G. LEJEUNE DIRICHLET,
PROF. A L'UNIVERSITÉ DE BERLIN.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 18 p. 259—274.

SUR L'USAGE DES SÉRIES INFINIES DANS LA THÉORIE DES NOMBRES.

Que toute progression arithmétique dont le premier terme et la raison sont des entiers sans diviseur commun, renferme une infinité de nombres premiers, c'est une proposition qui se présente, pour ainsi dire, d'elle-même, mais dont la démonstration rigoureuse n'en est pas moins sujette à de grandes difficultés. L'illustre LEGENDRE qui l'a employée comme lemme dans différentes recherches et particulièrement pour établir la belle loi de réciprocité qu'il avait découverte entre deux nombres premiers impairs quelconques, s'est aussi attaché à en donner la démonstration qui était en effet à désirer, à cause des nombreuses applications dont la proposition est susceptible. Cette démonstration dont le principe est très ingénieux, ne semble pas complète; en la considérant avec beaucoup d'attention, on reconnaît que l'auteur y fait usage d'un théorème qu'il ne fonde que sur l'induction, et qui n'est peut-être pas moins difficile à prouver que la proposition que l'auteur en déduit. Du moins les tentatives que j'ai faites pour compléter les recherches de LEGENDRE, ne m'ont pas réussi et j'ai été obligé de recourir à des moyens tout à fait différents. Je suis parvenu à établir la proposition dont il s'agit, en m'appuyant sur les propriétés d'une classe de séries infinies, qui ont beaucoup d'analogie avec celles qu'EULER considère dans le chap. XV. de son Introd. à l'Anal. de l'inf. Depuis que j'ai écrit le Mémoire qui contient cette démonstration*), et qui paraîtra dans le volume de l'Académie de Berlin, actuellement sous presse, j'ai continué à approfondir les propriétés des séries dont j'y ai fait usage. Ces nouvelles recherches m'ont fait reconnaître que la considération des séries de cette espèce constitue une méthode très féconde d'analyse indéterminée, et qui s'applique à des questions très variées. En attendant que je puisse achever un travail étendu sur cette matière, je vais indiquer rapidement quelques applications

*) S. 313 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

nouvelles de ce genre d'analyse. La méthode que j'emploie, me paraît surtout mériter quelque attention par la liaison qu'elle établit entre l'Analyse infinitésimale et l'Arithmétique transcendante, et j'espère que sous ce rapport elle pourra même intéresser les géomètres qui ne s'occupent pas spécialement des questions relatives aux propriétés des nombres.

La lettre q désignant un nombre premier positif $4\nu+3$, les nombres premiers positifs impairs et différents de q seront de deux espèces. Pour ceux de la première espèce que nous désignerons généralement par f , on a suivant la notation et un théorème connus :

$$\left(\frac{-q}{f}\right) = \left(\frac{f}{q}\right) = 1,$$

tandis que ceux de la seconde espèce, désignés par g , sont tels que :

$$\left(\frac{-q}{g}\right) = \left(\frac{g}{q}\right) = -1.$$

Soit de plus s une variable continue et positive, assujettie à rester supérieure à l'unité. Cela posé, on a évidemment ces trois équations :

$$(1) \quad \left\{ \begin{array}{l} H \frac{1}{1-\frac{1}{f^s}} \cdot H \frac{1}{1-\frac{1}{g^s}} = \Sigma \frac{1}{n^s}, \\ H \frac{1}{1-\frac{1}{f^s}} \cdot H \frac{1}{1+\frac{1}{g^s}} = \Sigma \left(\frac{n}{q}\right) \frac{1}{n^s}, \\ H \frac{1}{1-\frac{1}{f^{2s}}} \cdot H \frac{1}{1-\frac{1}{g^{2s}}} = \Sigma \frac{1}{n^{2s}}, \end{array} \right.$$

le signe de multiplication se rapportant à toutes les valeurs de f ou de g , et le signe sommatoire à toutes les valeurs de n positives, impaires et non-divisibles par q . On conclut des équations précédentes :

$$(2) \quad H \frac{1+\frac{1}{f^s}}{1-\frac{1}{f^s}} = \frac{\Sigma \frac{1}{n^s} \cdot \Sigma \left(\frac{n}{q}\right) \frac{1}{n^s}}{\Sigma \frac{1}{n^{2s}}}.$$

Comme l'on a :

$$1 + \frac{1}{f^s} = 1 + \frac{2}{f^s} + \frac{2}{f^{2s}} + \frac{2}{f^{3s}} + \dots,$$

on voit facilement que le premier membre de l'équation (2) peut être développé en une série de la forme:

$$(3) \quad \Sigma \frac{2^{\mu}}{m^{\mu}},$$

le signe Σ se rapportant à toutes les valeurs positives et impaires de m qui n'ont que des facteurs premiers de l'espèce f , et μ étant le nombre des diviseurs premiers inégaux de m .

Considérons maintenant les différentes formes quadratiques dont $-q$ est le déterminant. Soient:

$$(4) \quad ax^2+2bxy+cy^2, \quad a'x^2+2b'xy+c'y^2, \quad \dots$$

ces formes, les coefficients extrêmes étant positifs et jamais pairs à la fois, c'est-à-dire les formes qui constituent ce que M. GAUSS appelle *genus positivum propriè primitivum*.

Dans cette énumération des formes quadratiques, nous adoptons la classification de M. GAUSS, c'est-à-dire que nous regardons comme différentes deux formes qui ne présentent que ce que l'illustre auteur des *Disquisitiones arithmeticae* appelle l'équivalence impropre. LAGRANGE, qui le premier a fait voir que, pour un déterminant donné, il n'y a qu'un nombre fini de formes différentes, considère comme équivalentes deux expressions telles que:

$$ax^2+2bxy+cy^2, \quad a'x'^2+2b'x'y'+c'y'^2,$$

lorsqu'on peut passer de l'une à l'autre par une substitution de la forme:

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y',$$

les entiers $\alpha, \beta, \gamma, \delta$ étant tels que $\alpha\delta - \beta\gamma = \pm 1$. Cette condition est en effet suffisante pour que les deux formes représentent les mêmes nombres. Néanmoins, il y a de l'avantage à ne regarder les deux formes comme complètement équivalentes que dans le cas, où il y a une transformation de l'une dans l'autre pour laquelle on a $\alpha\delta - \beta\gamma = +1$. En adoptant cette notion de l'équivalence propre, on simplifie singulièrement un grand nombre de recherches et l'on conserve la concision dans beaucoup d'énoncés qui, faute d'y avoir égard, se trouveraient surchargés de restrictions. Il y a même des théorèmes qui paraissent isolés et restreints aux déterminants qui remplissent certaines conditions, dans la manière ordinaire de considérer les formes quadratiques, tandis qu'ils ne se présentent que comme des cas particuliers de propriétés générales communes aux formes de même déterminant quelconque, lorsqu'on envisage les choses sous le point de vue de M. GAUSS. On en voit un exemple

remarquable, si l'on rapproche le théorème, démontré dans la Théorie des nombres 4. part. §. VI, de celui qui fait l'objet de l'art. 252 des *Disq. arith.*

Il est d'ailleurs facile de passer de la classification de LEGENDRE à celle de M. GAUSS. Ce passage consiste simplement à attribuer l'un et l'autre signe aux coefficients moyens, en exceptant toutefois quelques formes particulières qui ne se doublent pas et qui sont précisément celles qui troublent la concision des propositions.

Supposons que, dans l'une quelconque des formes (4), on attribue aux indéterminées x et y des valeurs positives ou négatives, premières entre elles et telles que la valeur correspondante m du trinôme soit impaire et non-divisible par q . Il résulte des théorèmes connus que m n'aura que des diviseurs premiers de l'espèce f . Réciproquement, un nombre quelconque m qui n'a que de pareils diviseurs, peut toujours être exprimé par une ou par plusieurs des formes (4), x et y recevant des valeurs sans diviseur commun, et pourra l'être autant de fois par la totalité de ces formes qu'il y a d'unités dans la puissance $2^{\mu+1}$, μ désignant, comme plus haut, le nombre des diviseurs simples inégaux de m . Il suffit pour s'en assurer, de rapprocher les art. 180 L., 155, 156 et 105 des *Disq. arithm.* On conclut de là cette équation:

$$2\Sigma \frac{2^{\mu}}{m^2} = \Sigma \frac{1}{(ax^2+2bxy+cy^2)^2} + \Sigma \frac{1}{(a'x^2+2b'xy+c'y^2)^2} + \dots,$$

chacune des sommations indiquées dans le second membre s'étendant à tous les systèmes de valeurs positives ou négatives de x et y , premières entre elles et qui rendent le trinôme où elles sont substituées, impair et non-divisible par q . En comparant l'équation précédente aux équations (2) et (3), on aura:

$$(5) \quad 2\Sigma \frac{1}{n^2} \cdot \Sigma \left(\frac{n}{q}\right) \frac{1}{n^2} = \Sigma \frac{1}{n^{2\alpha}} \cdot \Sigma \frac{1}{(ax^2+2bxy+cy^2)^2} + \dots$$

Les termes du second membre peuvent prendre une forme plus simple. Le premier de ces termes, par exemple, est évidemment équivalent à l'expression:

$$\Sigma' \frac{1}{(ax^2+2bxy+cy^2)^2},$$

la double sommation indiquée par Σ' , se rapportant à tous les systèmes de valeurs positives ou négatives de x et y , qui remplissent la seule condition de rendre le trinôme impair et non-divisible par q .

Cette double sommation ne saurait être effectuée tant que la variable s reste indéterminée, mais le résultat devient extrêmement simple lorsque cette

variable surpasse infiniment peu l'unité. En posant $s = 1 + \varrho$, ϱ étant positif et infiniment petit, et exprimant la série double par une intégrale définie, on trouve assez facilement, surtout si l'on s'aide de considérations géométriques, que la valeur de la série est :

$$\frac{(q-1)}{2q\sqrt{q}} \cdot \frac{\pi}{e},$$

c'est-à-dire que le rapport de la série à l'expression précédente converge vers l'unité, lorsque ϱ converge vers zéro. Ce résultat étant indépendant des coefficients a , b , c , et ne renfermant que le déterminant commun à toutes les formes (4), dont nous désignerons le nombre par h , on conclut que le second membre de l'équation (5) est équivalent à :

$$h \frac{(q-1)}{2q\sqrt{q}} \cdot \frac{\pi}{e},$$

ϱ étant toujours considéré comme infiniment petit. D'un autre côté, on s'assure facilement que le facteur $\Sigma \frac{1}{n^s}$ du premier membre a pour valeur :

$$\frac{q-1}{2q} \cdot \frac{1}{e},$$

tandis que l'autre facteur converge vers la limite finie $\Sigma \left(\frac{n}{q}\right) \frac{1}{n}$. On a donc l'égalité :

$$h = \frac{2\sqrt{q}}{\pi} \Sigma \left(\frac{n}{q}\right) \frac{1}{n} = \frac{2\sqrt{q}}{\pi} S.$$

Pour obtenir le nombre h , tout se réduit donc à déterminer S ; à cet effet

multiplions par $\frac{1}{1 - \left(\frac{2}{q}\right) \frac{1}{2}}$, il viendra ainsi :

$$\frac{1}{1 - \left(\frac{2}{q}\right) \frac{1}{2}} S = \Sigma \left(\frac{n}{q}\right) \frac{1}{n},$$

le signe se rapportant maintenant à toutes les valeurs entières de n , paires ou impaires, à partir de $n = 1$, à l'exception de celles qui sont divisibles par q . Pour effectuer cette sommation, nous aurons recours aux belles formules de M. GAUSS. Désignant généralement par a et b (il est sans doute inutile d'avertir qu'il ne faut pas confondre cette signification des lettres a et b avec celle que nous leur avons donnée plus haut) les résidus et les non-résidus quadratiques de q moindres que ce nombre, et par n un entier quelconque non-divisible par q , on a :

$$\Sigma \sin \frac{2an\pi}{q} - \Sigma \sin \frac{2bn\pi}{q} = \left(\frac{n}{q}\right) \sqrt{q^*}.$$

les sommations se rapportant à toutes les valeurs de a ou de b . En introduisant cette expression de $\left(\frac{n}{q}\right)$ dans l'équation précédente, il viendra :

$$\frac{\sqrt{q}}{1 - \left(\frac{2}{q}\right) \frac{1}{2}} S = \Sigma \Sigma \frac{1}{n} \sin \frac{2an\pi}{q} - \Sigma \Sigma \frac{1}{n} \sin \frac{2bn\pi}{q}.$$

Les sommations se rapportent l'une à a ou b , l'autre à n , et il n'est plus nécessaire maintenant d'exclure les valeurs de n divisibles par q , le sinus s'évanouissant pour ces valeurs particulières de n . En commençant par la sommation relative à n , qui peut s'effectuer au moyen de l'équation connue :

$$\frac{\pi - z}{2} = \Sigma \frac{1}{n} \sin nz,$$

qui a lieu tant que z reste compris entre 0 et 2π , on aura :

$$\frac{\sqrt{q}}{1 - \left(\frac{2}{q}\right) \frac{1}{2}} S = \Sigma \left(\frac{\pi - a\pi}{2} - \frac{a\pi}{q} \right) - \Sigma \left(\frac{\pi - b\pi}{2} - \frac{b\pi}{q} \right)$$

et par suite, en remarquant qu'il y a autant de valeurs de a que de b :

$$S = \left[1 - \left(\frac{2}{q}\right) \frac{1}{2} \right] \frac{\pi}{q\sqrt{q}} (\Sigma b - \Sigma a).$$

L'expression de h deviendra donc :

$$h = 2 \left[1 - \left(\frac{2}{q}\right) \frac{1}{2} \right] \frac{\Sigma b - \Sigma a}{q}.$$

Le nombre premier q peut présenter deux cas. S'il est de la forme $8r+3$, on a $\left(\frac{2}{q}\right) = -1$, et s'il est compris dans la forme $8r+7$, $\left(\frac{2}{q}\right) = +1$. On a donc pour le nombre h des formes quadratiques différentes dont le déterminant est $-q$:

$$h = 3 \frac{\Sigma b - \Sigma a}{q}, \quad q = 8r+3 \quad \text{ou} \quad h = -\frac{\Sigma b - \Sigma a}{q}, \quad q = 8r+7.$$

Ce double résultat s'accorde avec l'élégant théorème que M. JACOBI a

*) Ce théorème et les théorèmes analogues que nous emploierons plus bas, ont été énoncés dans les *Disq. arithm.* art. 356, mais la démonstration complète qui présentait de grandes difficultés à cause de l'ambiguïté de signe du radical, n'a été donnée que postérieurement par l'illustre auteur dans un mémoire spécial. Comment. societ. Gotting. recentiores. Vol. I^o). J'en ai donné une autre, fondée sur des principes entièrement différents. Voyez les Mémoires de Berlin, année 1835, ou le Journal de CRELLE, tome XVII. *) On pourra se convaincre par les nombreuses applications que nous ferons de ces formules, combien il importait de faire cesser l'ambiguïté du signe, qui affecterait également tous les résultats que ces formules contiennent à faire obtenir.

1) Gauss' Werke, Band II, S. 9. 2) S. 237 und S. 237 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

énoncé, il y déjà plusieurs années*). Pour faire coïncider les deux résultats, il faut remarquer d'abord que l'illustre géomètre a adopté la classification de LEGENDRE, de sorte que le nombre des formes qu'il désigne par N , est tel qu'on a $h = 2N - 1$. En effet, parmi les formes du déterminant $= q$, il n'y a qu'une seule forme ambiguë qui est $x^2 + qy^2$, et qui ne se double pas en passant de la classification de LEGENDRE à celle de M. GAUSS. En second lieu, il faut faire attention que dans le cas où q est de la forme $8r + 3$, M. JACOBI considère des formes à coefficient moyen impair, comme LEGENDRE l'avait déjà fait dans sa Table, ce qui réduit le nombre des formes au tiers.

Si l'on somme la série S sans introduire le facteur $\frac{1}{1 - \left(\frac{2}{q}\right)^{\frac{1}{2}}}$, on arrive à cet autre résultat plus simple que le précédent:

$$h = A - B = 2A - \frac{1}{2}(q-1),$$

où A et B désignent respectivement combien il y a de résidus et de non-résidus quadratiques de q moindres que $\frac{1}{2}q$.

Soit p un nombre premier $4r + 1$, l'unité exceptée, et partageons en deux classes les nombres premiers impairs et différents de p . Désignons généralement par f ceux pour lesquels on a:

$$\left(\frac{-p}{f}\right) = \left(\frac{f}{p}\right)(-1)^{\frac{f-1}{2}} = 1,$$

et par g ceux qui satisfont à la condition:

$$\left(\frac{-p}{g}\right) = \left(\frac{g}{p}\right)(-1)^{\frac{g-1}{2}} = -1.$$

On aura alors, comme dans le cas déjà considéré:

$$H \frac{1}{1 - \frac{1}{f^x}} \cdot H \frac{1}{1 - \frac{1}{g^x}} = \sum \frac{1}{n^x},$$

$$H \frac{1}{1 - \frac{1}{f^x}} \cdot H \frac{1}{1 + \frac{1}{g^x}} = \sum (-1)^{\frac{n-1}{2}} \left(\frac{n}{p}\right) \frac{1}{n^x},$$

$$H \frac{1}{1 - \frac{1}{f^{2x}}} \cdot H \frac{1}{1 - \frac{1}{g^{2x}}} = \sum \frac{1}{n^{2x}}.$$

*) *Observatio arithmetica etc.* Vol. IX. du Journal de CRELLE. Voyez aussi le compte rendu des séances de l'Académie de Berlin, Oct. 1837, ainsi que les *Disq. arithm.* art. 306, X et surtout la note relative à cet art., à la fin de l'ouvrage, où M. GAUSS annonce des recherches sur le même sujet, mais qui n'ont pas été publiées jusqu'à présent.

et par suite :

$$\Sigma \frac{1}{n^{2s}} \cdot \Pi \frac{1 + \frac{1}{f^s}}{1 - \frac{1}{f^s}} = \Sigma \frac{1}{n^s} \cdot \Sigma (-1)^{\frac{n-1}{2}} \left(\frac{n}{p}\right) \frac{1}{n^s},$$

le signe Σ se rapportant aux valeurs de n impaires et non-divisibles par p , à partir de $n = 1$. Cette équation prendra comme précédemment cette autre forme :

$$(6) \quad \Sigma \frac{1}{n^{2s}} \cdot \Sigma \frac{2^\mu}{m^s} = \Sigma \frac{1}{n^s} \cdot \Sigma (-1)^{\frac{n-1}{2}} \left(\frac{n}{p}\right) \frac{1}{n^s},$$

m désignant tous les nombres impairs qui n'ont que des diviseurs premiers de l'espèce f , et μ le nombre de ces diviseurs premiers inégaux. On a par suite :

$$(7) \quad \Sigma' \frac{1}{(ax^2 + 2bxy + cy^2)^s} + \Sigma' \frac{1}{(a'x^2 + 2b'xy + c'y^2)^s} + \dots = 2\Sigma \frac{1}{n^s} \cdot \Sigma (-1)^{\frac{n-1}{2}} \left(\frac{n}{p}\right) \frac{1}{n^s},$$

où le premier membre a autant de termes qu'il y a de formes pour le déterminant $-p$, et les sommations indiquées par Σ' s'étendant à tous les systèmes de valeurs positives ou négatives de x et y , qui rendent le trinôme sous le signe de sommation premier à $2p$. En faisant $s = 1 + \varrho$, et désignant par h le nombre des formes, le premier membre deviendra :

$$\frac{h(p-1)}{2p} \frac{\pi}{p^{\varrho}}$$

et l'on aura en même temps :

$$\Sigma \frac{1}{n^s} = \frac{p-1}{2p} \cdot \frac{1}{p^{\varrho}}.$$

On conclut de là :

$$h = \frac{2\sqrt{p}}{\pi} \Sigma (-1)^{\frac{n-1}{2}} \left(\frac{n}{p}\right) \frac{1}{n} = \frac{2\sqrt{p}}{\pi} S.$$

Pour obtenir la série qui entre dans cette expression de h , nous aurons recours à la formule de M. GAUSS :

$$\Sigma \cos \frac{2an\pi}{p} - \Sigma \cos \frac{2bn\pi}{p} = \left(\frac{n}{p}\right) \sqrt{p},$$

dans laquelle n est un nombre quelconque non-divisible par p , et les sommations s'étendant à tous les résidus quadratiques a ou à tous les non-résidus quadratiques b de p qui sont moindres que ce nombre premier. Au moyen de ce théorème, il viendra :

$$\{p\} S = \Sigma \Sigma (-1)^{\frac{n-1}{2}} \frac{1}{n} \cos \frac{2an\pi}{p} - \Sigma \Sigma (-1)^{\frac{n-1}{2}} \frac{1}{n} \cos \frac{2bn\pi}{p},$$

où il est permis de ne plus exclure les valeurs de n divisibles par p , car il est

facile de voir qu'on introduit ainsi les mêmes termes étrangers dans chacune des deux séries doubles qui sont précédées de signes opposés. La sommation relative à n peut être effectuée au moyen de la formule connue :

$$q(z) = \Sigma(-1)^{\frac{n-1}{2}} \frac{\cos n z}{n} (*),$$

dont le premier membre est une fonction discontinue de z , et qui a respectivement pour valeur $\frac{1}{4}\pi$, $-\frac{1}{4}\pi$, ou $\frac{1}{4}\pi$ selon que z est compris entre 0 et $\frac{1}{2}\pi$, entre $\frac{1}{2}\pi$ et $\frac{3}{2}\pi$, ou enfin entre $\frac{3}{2}\pi$ et 2π . Si donc on désigne par A , A' , A'' les nombres des valeurs de a comprises entre 0 et $\frac{1}{4}p$, $\frac{1}{4}p$ et $\frac{3}{4}p$, $\frac{3}{4}p$ et p , et par B , B' , B'' les nombres analogues relatifs aux valeurs de b , l'expression de S deviendra :

$$S = \frac{\pi}{4\sqrt{p}} (A - A' + A'' - B + B' - B'').$$

et comme l'on a en vertu de propriétés connues du nombre premier p :

$$A = A'', \quad B = B'', \quad A + A' + A'' = B + B' + B'' = \frac{1}{2}(p-1),$$

on conclut :

$$S = \frac{\pi}{4\sqrt{p}} (A - B).$$

On a donc cette formule très simple pour déterminer le nombre h des formes quadratiques dont le déterminant est $-p$:

$$h = 2(A - B) = 4A - \frac{1}{2}(p-1).$$

On sait que ces formes sont de deux espèces, les unes ne représentant que des nombres impairs $4\nu+1$, et les autres que des nombres impairs $4\nu+3$. Désignons par k et l les nombres des formes qui appartiennent respectivement au premier et au second de ces deux genres. Pour déterminer k et l , on remarquera que l'égalité (6) reste exacte, en y modifiant les signes comme il suit :

$$\Sigma \frac{1}{n^{2s}} \cdot \Sigma(-1)^{\frac{m-1}{2}} \frac{2^u}{m^s} = \Sigma(-1)^{\frac{m-1}{2}} \frac{1}{n^s} \cdot \Sigma\left(\frac{n}{p}\right) \frac{1}{n^s}.$$

L'équation qui en dérive et qui est analogue à l'équation (7), ne diffère de cette dernière qu'en ce que les séries doubles désignées par Σ' , sont précédées du signe $-$, lorsque la forme quadratique qui s'y trouve sous le signe Σ' , appartient au second genre. On aura donc, en posant toujours $s = 1 + \varrho$:

$$(k-l) \frac{(p-1)}{2p\sqrt{p}} \cdot \frac{\pi}{\varrho}$$

*) Théorie analytique de la chaleur, p. 175.

pour la valeur du premier membre, et comme le second membre reste évidemment fini, on conclut:

$$k-l = 0,$$

ce qui donne:

$$k = l = A - B = 2A - \frac{1}{2}(p-1).$$

Les deux genres contiennent donc chacun le même nombre de formes.

Ce résultat renferme le théorème déjà cité de la Théorie des Nombres. En effet, lorsque p est de la forme $8\nu+1$, les deux formes ambiguës:

$$x^2 + \nu y^2, \quad 2x^2 + 2xy + \frac{1}{2}(p+1)y^2,$$

qui ne se doublent pas en passant à la classification de M. GAUSS, appartiennent l'une et l'autre au premier genre. On a donc, entre les signes de LEGENDRE et ceux que nous venons d'employer, ces relations:

$$k = 2(M-2)+2, \quad l = 2N.$$

d'où l'on conclut $M = N+1$.

Par une analyse entièrement semblable à celle que nous avons appliquée, dans ce qui précède, aux déterminants $-q$ et $-\nu$, on peut obtenir le nombre des formes quadratiques dont le déterminant est un nombre quelconque, positif ou négatif, premier ou composé. On trouve ainsi les théorèmes suivants:

— q étant toujours un nombre premier $4\nu+3$, désignons par A et par B respectivement combien il y a de résidus et de non-résidus quadratiques de q entre les limites $\frac{1}{5}q$ et $\frac{3}{5}q$. Cela posé, le nombre des formes dont le déterminant est $-2q$, sera exprimé par:

$$2(A-B),$$

ces formes étant d'ailleurs également réparties entre les deux genres qui existent pour ce cas."

— p étant un nombre premier $4\nu+1$, soient A et B respectivement les nombres des résidus et des non-résidus quadratiques compris entre 0 et $\frac{1}{5}p$; soient de même A' et B' les nombres des résidus et des non-résidus qui tombent entre $\frac{3}{5}p$ et $\frac{1}{2}p$. Cela posé, le nombre des formes quadratiques, ayant $-2p$ pour déterminant, sera exprimé par:

$$2(A-B-A'+B'),$$

ces formes étant d'ailleurs également réparties entre les deux genres."

— Les lettres p et q conservant la signification précédente, désignons généralement par a les nombres inférieurs et premiers à pq , qui sont tels que $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$, et par b les nombres analogues qui remplissent la condition

$\left(\frac{b}{p}\right) = -\left(\frac{b}{q}\right)$. Cela posé, l'expression du nombre des formes quadratiques dont le déterminant est $-pq$, sera:

$$\frac{\Sigma b - \Sigma a}{pq} \quad \text{ou} \quad 3 \frac{\Sigma b - \Sigma a}{pq}.$$

selon que l'on aura $pq \equiv 7$ ou $-3 \pmod{8}$, ces formes étant toujours également partagées entre les deux genres.* (Ce théorème est susceptible d'un autre énoncé plus simple, comme celui donné ci-dessus pour le déterminant $-q$.)

Et ainsi de suite.

Lorsque le déterminant est un nombre positif D , l'analyse qui fait connaître le nombre des formes quadratiques différentes, exige une attention toute particulière à cause des nouvelles conditions auxquelles il faut avoir égard dans les sommations doubles que nous avons désignées par Σ' . Ces conditions qui s'ajoutent à celles qui ont lieu pour les déterminants négatifs, consistent 1^o, en ce que les valeurs de x et de y doivent être choisies de manière à rendre le trinôme $ax^2 + 2bxy + cy^2$ positif, et 2^o, en ce qu'il ne faut employer qu'un seul des systèmes de valeurs de x et de y , en nombre infini, qui se déduisent les uns des autres, au moyen des formules:

$$x' = xt - (bx + cy)u, \quad y' = yt + (ax + by)u,$$

t et u désignant tous les nombres positifs ou négatifs satisfaisant à l'équation:

$$(8) \quad t^2 - Du^2 = 1.$$

Cette circonstance introduit dans l'expression de la série double le facteur:

$$\log(T + U\sqrt{D}).$$

T et U désignant les plus petits nombres (à l'exception de 1 et 0) qui résolvent l'équation précédente, en sorte que ce logarithme joue ici le même rôle que le nombre π dans le cas des déterminants négatifs. D'un autre côté, la série analogue à celles que nous avons désignées par:

$$\Sigma \left(\frac{n}{q}\right) \frac{1}{n} \quad \text{et} \quad \Sigma (-1)^{\nu(n-1)} \left(\frac{n}{p}\right) \frac{1}{n}.$$

et que renferme l'autre membre de l'équation, sera également exprimée par un logarithme tel que $\log(T' + U'\sqrt{D})$, T' et U' étant la solution de l'équation (8), qui se déduit de l'application des fonctions circulaires.* Or, on a en vertu d'un

* S. 343 dieser Ausgabe von Lejeune Dirichlet's Werken. K.

théorème connu :

$$T^{\lambda} + U^{\lambda} \sqrt{D} = (T + U \sqrt{D})^{\lambda},$$

λ étant un entier et par conséquent :

$$\lambda = \frac{\log(T^{\lambda} + U^{\lambda} \sqrt{D})}{\log(T + U \sqrt{D})}.$$

C'est donc de cet entier λ que dépend le nombre des formes, mais l'expression de cette dépendance présente quelque légère différence selon les différentes formes dont le déterminant D est susceptible.

L'analyse que nous venons d'indiquer d'une manière rapide, en même temps qu'elle détermine le nombre des formes, a l'avantage de simplifier singulièrement plusieurs théories très importantes déjà connues, mais qui n'avaient été établies que par des méthodes très compliquées. De ce genre sont celles qui se résument dans les beaux théorèmes démontrés par M. GAUSS dans les art. 252, 261 et 287, III. des *Disq. arith.*, et dont le dernier surtout exigeait jusqu'à présent le concours d'un grand nombre de recherches très étendues. (Voyez la fin de l'art. 287.) Ce même théorème résulte aussi d'une combinaison très simple de la loi de réciprocité avec la proposition sur la progression arithmétique, mais ce moyen de démonstration ne diffère pas au fond de celui que nous venons d'indiquer, du moins lorsque, pour établir que toute progression arithmétique renferme une infinité de nombres premiers, on a recours aux séries, comme nous l'avons fait dans le mémoire cité plus haut.

Les théorèmes qui déterminent le nombre des formes quadratiques, renferment implicitement un grand nombre de propositions qui peuvent s'énoncer indépendamment de la théorie de ces formes, et qui seraient peut-être très difficiles à démontrer sans le secours combiné de nos séries et des formules de M. GAUSS. Il résulte, par exemple, de ce qu'on a vu plus haut que pour un nombre premier $q = 4\nu + 3$, la somme des non-résidus quadratiques surpasse toujours celle des résidus^{*)}, que pour un nombre premier $p = 4\nu + 1$, il y a toujours un plus grand nombre de résidus que de non-résidus, moindres que $\frac{1}{2}p$, etc. On peut encore augmenter le nombre de ces propositions, les séries

^{*)} On a encore $A > B$, A et B désignant comme ci-dessus combien il y a de résidus et de non-résidus de q , au-dessous de $\frac{1}{2}q$. Dans un article du Bulletin de M. DE FÉRSSAC (Mars 1831, p. 137), où M. CAUVY énonce un théorème très remarquable sur les nombres premiers $4\nu + 3$, ce célèbre analyste distingue deux cas selon que $A > B$ ou $A < B$. Ce qu'on a prouvé plus haut, montre que le second cas ne saurait avoir lieu et fait cesser l'indétermination que le théorème de M. CAUVY semblait présenter.

que nous avons considérées étant susceptibles d'être sommées dans plusieurs cas sans que l'on y suppose $s = 1$. C'est ce qui arrive, par exemple, pour la série $\Sigma \binom{n}{p} \frac{1}{n^2}$, le signe Σ se rapportant à toutes les valeurs entières de n , à partir de $n = 1$, à l'exclusion de celles qui sont divisibles par p . En effectuant cette sommation, on arrive à la conclusion que pour un nombre premier $p = 4\nu + 1$, on a toujours $\Sigma a^2 > \Sigma b^2$.

Des considérations du même genre peuvent aussi servir à faire cesser l'indétermination que présentent les formules qui donnent une solution de l'équation $t^2 - Du^2 = 1$, au moyen des fonctions circulaires, et qui ont été publiées par M. JACOBI et par moi*). Pour en donner un exemple, supposons $D = p$. On a alors:

$$k\sqrt[p]{p+h} = \frac{2}{\sqrt[p]{p}} \Pi \left(1 - e^{\frac{2a\pi}{p}} \sqrt[p]{-1} \right) = \frac{2^{1/p+1}}{\sqrt[p]{p}} \Pi \sin \frac{a\pi}{p},$$

$$k\sqrt[p]{p-h} = \frac{2}{\sqrt[p]{p}} \Pi \left(1 - e^{\frac{2b\pi}{p}} \sqrt[p]{-1} \right) = \frac{2^{1/p+1}}{\sqrt[p]{p}} \Pi \sin \frac{b\pi}{p},$$

le signe Π se rapportant à toutes les valeurs de a ou de b , et les entiers h et k satisfaisant à l'équation:

$$h^2 - pk^2 = -4.$$

Il y a des questions qui exigent qu'on connaisse les signes dont les valeurs de k et h , tirées des équations précédentes, sont affectées.

Il est évident que la valeur de k est positive, mais la détermination du signe de h présente des difficultés. Pour y parvenir, on remarquera que h sera positif ou négatif, selon que le rapport:

$$\frac{k\sqrt[p]{p+h}}{k\sqrt[p]{p-h}}$$

sera supérieur ou inférieur à l'unité. Tout se réduit donc à voir si

$$\log \left(\frac{k\sqrt[p]{p+h}}{k\sqrt[p]{p-h}} \right)$$

est positif ou négatif. Le développement en série donne:

$$\log \left(\frac{k\sqrt[p]{p+h}}{k\sqrt[p]{p-h}} \right) = -\Sigma \frac{1}{n} \left(\Sigma e^{\frac{2an\pi}{p}} \sqrt[p]{-1} - \Sigma e^{\frac{2bn\pi}{p}} \sqrt[p]{-1} \right).$$

*) Compte rendu de l'Académie de Berlin, Octobre 1837. Tome XVII du Journal de CRELLE. 1)

1) S. 343 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

la sommation relative à n s'étendant à toutes les valeurs entières et positives. Or, la différence:

$$\sum e^{\frac{2\alpha n\pi}{p}\sqrt{-1}} - \sum e^{\frac{2\beta n\pi}{p}\sqrt{-1}}$$

s'évanouit lorsque n est divisible par p ; dans les autres cas elle devient, par les formules de M. GAUSS, $\left(\frac{n}{p}\right)\sqrt{p}$. On a donc simplement:

$$\log\left(\frac{k\sqrt{p+h}}{k\sqrt{p-h}}\right) = -\sqrt{p}\sum\left(\frac{n}{p}\right)\frac{1}{n}.$$

où il faut exclure les valeurs de n divisibles par p .

La série renfermée dans le second membre étant la limite de $\sum\left(\frac{n}{p}\right)\frac{1}{n^s}$, lorsque s converge vers l'unité, et cette dernière pouvant se décomposer en une infinité de facteurs tous positifs, comme il suit:

$$\frac{1}{1-\left(\frac{2}{p}\right)\frac{1}{2^s}} \cdot \frac{1}{1-\left(\frac{3}{p}\right)\frac{1}{3^s}} \cdot \frac{1}{1-\left(\frac{5}{p}\right)\frac{1}{5^s}} \dots$$

où entre toute la série des nombres premiers, le seul nombre p excepté, on conclut que $\sum\left(\frac{n}{p}\right)\frac{1}{n}$ a une valeur positive, et partant que le signe de h qu'il s'agissait de déterminer, est négatif.

Je terminerai cette note, en montrant le parti qu'on peut tirer des séries précédentes, pour déterminer les expressions-limites des valeurs moyennes de certaines fonctions très irrégulières, relatives aux propriétés des nombres. (Voyez pour la définition des valeurs moyennes des fonctions de ce genre, les *Disq. arithm.* art. 301.) Dans un Mémoire récemment lu à l'Académie de Berlin*), je me suis attaché à établir quelques principes desquels on peut déduire ces expressions-limites ou lois finales, dont la connaissance est très utile dans différentes recherches. J'ai fait l'application de ces principes à la démonstration de la formule remarquable**) que LEGENDRE a donnée pour exprimer d'une manière très approchée combien il y a de nombres premiers au-dessous d'une limite quelconque, mais très grande, et à d'autres questions du même genre. J'ai trouvé, par exemple, que la formule très-simple:

$$\log n + 2C,$$

*) *Compte rendu pour le mois de Février 1838.* †)

**) qui n'est exacte que dans son premier terme, la véritable expression-limite étant $\sum \frac{1}{\log(n)}$ ‡).

†) S. 351 dieser Ausgabe von G. Lejeune Dirichlet's Werken. ‡) Anmerkung von Lejeune Dirichlet's Hand in dem an Gauss geschickten Exemplar. K.

C désignant une constante connue (EULERI Calc. diff. p. 444), exprime avec d'autant plus d'exactitude que n est plus grand, la valeur moyenne du nombre des diviseurs de l'entier n , et qu'on a pareillement pour la somme moyenne de ces mêmes diviseurs :

$$\frac{1}{6}\pi^2 n - \frac{1}{2}.$$

Ces résultats ont été conclus de la série connue de LAMBERT et d'une autre série analogue. Ils pourraient aussi se déduire des séries considérées plus haut. Voici maintenant un nouveau résultat qu'on tire de ces dernières séries. Soit $f(n)$ la fonction de n , qui indique de combien de manières le nombre n peut se décomposer en deux facteurs premiers entre eux. On a, comme l'on sait, $f(n) = 2^\lambda$, λ désignant le nombre des diviseurs premiers inégaux de n . Cela posé, on trouve facilement :

$$\sum \frac{f(n)}{n^s} = \frac{g^2(s)}{g(2s)},$$

où l'on a fait $g(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \dots$, et la sommation devant s'étendre à toutes les valeurs entières de n , à partir de $n = 1$. En posant, comme plus haut, $s = 1 + \rho$, et développant le second membre suivant les puissances ascendantes de ρ , il viendra :

$$\sum \frac{f(n)}{n^{1+\rho}} = \frac{6}{\pi^2} \left[\frac{1}{\rho^2} + \left(\frac{12C'}{\pi^2} + 2C \right) \frac{1}{\rho} + \dots \right].$$

La constante C est la même que ci-dessus, et C' désigne la série :

$$\frac{\log 2}{2^2} + \frac{\log 3}{3^2} + \frac{\log 4}{4^2} + \dots$$

Au moyen de la méthode développée dans le mémoire cité, on trouve sur le champ que l'expression-limite de la valeur moyenne de $f(n)$ est celle-ci :

$$\frac{6}{\pi^2} \left(\log n + \frac{12C'}{\pi^2} + 2C \right).$$

Les formules remarquables que M. GAUSS a indiquées dans les art. 301 et suiv. de son bel ouvrage, peuvent être obtenues par une analyse du même genre. Supposons, par exemple, qu'il s'agisse d'obtenir la valeur moyenne du nombre des genres pour le déterminant $-n$, nombre que nous désignerons par $F(n)$. Si l'on compare l'art. 231, où tous les caractères complets assignables *a priori* sont énumérés, avec les art. 261 et 287, où l'illustre auteur fait voir qu'il n'y a que la moitié de ces caractères qui correspondent à des genres réellement existants, on trouvera facilement les cinq équations qui

suivent et dans lesquelles on a posé, pour abrégér :

$$\psi(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \dots, \quad \chi(s) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \dots;$$

$$\left\{ \begin{array}{l} \frac{2}{8^s - 4^s} \cdot \frac{\psi^2(s)}{\psi(2s)} = \Sigma \frac{F(n)}{n^s}, \quad n = 8v, \\ \frac{1}{4^s} \cdot \frac{\psi^2(s)}{\psi(2s)} = \Sigma \frac{F(n)}{n^s}, \quad n = 8v+4, \\ \frac{1}{2^s} \cdot \frac{\psi^2(s)}{\psi(2s)} = \Sigma \frac{F(n)}{n^s}, \quad n = 4v+2, \\ \frac{1}{2} \cdot \frac{\psi^2(s) + \chi^2(s)}{\psi(2s)} = \Sigma \frac{F(n)}{n^s}, \quad n = 4v+1, \\ \frac{1}{4} \cdot \frac{\psi^2(s) - \chi^2(s)}{\psi(2s)} = \Sigma \frac{F(n)}{n^s}, \quad n = 4v+3, \end{array} \right.$$

les sommations se rapportant à toutes les valeurs positives et entières de n comprises dans la forme linéaire indiquée à côté. En faisant comme plus haut $s = 1 + \rho$, on trouve que l'expression-limite de la valeur moyenne de $F(n)$, est, suivant les cinq formes qu'on vient d'énumérer :

$$\begin{aligned} & \frac{8}{\pi^2} \left(\log n + \frac{12C'}{\pi^2} + 2C - \frac{2}{3} \log 2 \right), \\ & \frac{4}{\pi^2} \left(\log n + \frac{12C'}{\pi^2} + 2C - \frac{2}{3} \log 2 \right), \\ & \frac{4}{\pi^2} \left(\log n + \frac{12C'}{\pi^2} + 2C + \frac{1}{3} \log 2 \right), \\ & \frac{4}{\pi^2} \left(\log n + \frac{12C'}{\pi^2} + 2C + \frac{1}{3} \log 2 \right), \\ & \frac{2}{\pi^2} \left(\log n + \frac{12C'}{\pi^2} + 2C + \frac{1}{3} \log 2 \right), \end{aligned}$$

et comme sur huit entiers consécutifs quelconques il y en a respectivement

$$1, 1, 2, 2, 2,$$

qui sont compris dans ces cinq formes :

$$8v, 8v+4, 4v+2, 4v+1, 4v+3,$$

on conclut que l'expression-limite de la valeur moyenne du nombre des genres pour un déterminant $-n$, dont on ne désigne pas la forme linéaire, est la somme des expressions précédentes respectivement multipliées par les fractions $\frac{1}{8}, \frac{1}{8}, \frac{2}{3}, \frac{2}{3}, \frac{2}{3}$. On trouve ainsi :

$$\frac{4}{\pi^2} \left(\log n + \frac{12C'}{\pi^2} + 2C - \frac{1}{6} \log 2 \right),$$

ce qui coïncide avec le résultat de M. GAUSS.

Berlin, au mois de mai 1838.

SUR UNE NOUVELLE MÉTHODE
POUR LA DÉTERMINATION DES INTÉGRALES
MULTIPLÉS.

PAR

G. LEJEUNE DIRICHLET.

SUR UNE NOUVELLE MÉTHODE POUR LA DÉTERMINATION DES INTÉGRALES MULTIPLES.

[Communication faite dans la séance du lundi 4 février 1839.]

On sait que l'évaluation ou même la réduction des intégrales multiples présente généralement de très grandes difficultés, lorsque les inégalités de condition qui définissent l'étendue des intégrations, renferment à la fois plusieurs des variables. En m'occupant de quelques questions de physique mathématique qui dépendent, en dernière analyse, de l'évaluation d'une classe d'intégrales multiples d'un ordre indéfini, j'ai été conduit à une méthode qui paraît diminuer, dans beaucoup de cas, les difficultés dont je viens de parler. Cette méthode consiste simplement à multiplier l'expression qu'il s'agit d'intégrer par un facteur dont la valeur est égale à l'unité dans l'étendue que les intégrations doivent embrasser, et qui s'évanouit en dehors de cette étendue. L'expression différentielle ainsi modifiée, pouvant être intégrée entre des limites constantes et très simples, telles que 0 et ∞ , ou $-\infty$ et ∞ , la question sera le plus souvent beaucoup plus facile à traiter. C'est ce procédé que je vais appliquer à quelques problèmes particuliers. Pour premier exemple, je choisirai la question si célèbre de l'attraction des ellipsoïdes homogènes. La méthode appliquée à ce problème présente cela de remarquable, que la solution pour les deux cas d'un point extérieur et d'un point intérieur, qu'on avait toujours ramenés du premier au second, ou traités par des moyens tout-à-fait différents, résulte d'une analyse uniforme, qui s'étend généralement à toute loi d'attraction proportionnelle à une puissance quelconque entière ou fractionnaire de la distance. La même analyse ramène ce problème aux quadratures, lorsque la densité, au lieu d'être constante, est une fonction quelconque rationnelle et entière des trois coordonnées rectangulaires; mais, pour plus de simplicité, je supposerai la densité constante et égale à l'unité.

Soient x, y, z , les coordonnées d'un point quelconque de la masse attirante, a, b, c celles du point attiré. Posons: $\varrho^2 = (x-a)^2 + (y-b)^2 + (z-c)^2$ et soit $\frac{1}{\varrho^p}$ la loi de l'attraction, la constante p étant supposée comprise entre 2 et 3, cas auquel il est facile de ramener tous les autres. Cela posé, la question se réduit à déterminer l'intégrale triple:

$$(1) \quad -\frac{1}{p-1} \iiint \frac{dx dy dz}{\varrho^{p-1}} \quad \left(\left(\frac{x}{a}\right)^2 + \left(\frac{y}{b}\right)^2 + \left(\frac{z}{c}\right)^2 < 1 \right)$$

dont le coefficient différentiel pris par rapport à a , donne la composante de l'attraction parallèle à l'axe des x , que je désignerai par A . Or, comme l'intégrale:

$$\frac{2}{\pi} \int_0^{\frac{\pi}{2}} \frac{\sin g}{g} \cos g g dg$$

est égale à l'unité ou à zéro, suivant que la constante positive g est inférieure ou supérieure à l'unité, on conclut que l'intégrale (1) est la partie réelle de celle-ci:

$$-\frac{2}{\pi(p-1)} \int_0^{\frac{\pi}{2}} \frac{\sin g}{g} dg \iiint e^{i \left[\left(\frac{x}{a}\right)^2 + \left(\frac{y}{b}\right)^2 + \left(\frac{z}{c}\right)^2 \right] g^2} \frac{dx dy dz}{\varrho^{p-1}},$$

les intégrations par rapport aux variables x, y, z pouvant maintenant s'étendre depuis $-\infty$ jusqu'à ∞ . Pour obtenir l'intégrale triple relative à ces variables, on exprimera la fraction $\frac{1}{\varrho^{p-1}}$ ou $\frac{1}{(\varrho^2)^{\frac{p-1}{2}}}$ par une intégrale définie, au moyen de la formule connue d'EULER:

$$(2) \quad \int_0^{\frac{\pi}{2}} \rho^{\psi} \psi^{r-1} \psi^{r-1} d\psi = \frac{\Gamma(q) e^{\frac{1}{2} \pi \Gamma^{-1}}}{q^r}$$

que M. POISSON a démontrée et qui suppose les constantes q et r positives, et de plus $r < 1$. Il viendra ainsi, en remplaçant ϱ^2 par sa valeur:

$$-\frac{2}{\pi} \frac{e^{-\frac{1}{2} \pi (p-1) \Gamma^{-1}}}{(p-1) \Gamma(\frac{1}{2}(p-1))} \int_0^{\frac{\pi}{2}} \frac{\sin g}{g} dg \int_0^{\frac{\pi}{2}} \psi^{\frac{1}{2}(p-1)-1} e^{(a^2+b^2+c^2)\psi} d\psi \cdot U,$$

U designant, pour abrégér, le produit de trois intégrales simples, dont celle relative à x est, en vertu d'une formule connue qui dérive de l'équation (2):

$$\int_{-\infty}^{+\infty} \rho^{\left(\left(\psi + \frac{q}{a^2} \right) x^2 - 2ax \right)} |1|^{-1} dx = \frac{1 + \sqrt{-1}}{12} \cdot \sqrt{\frac{\alpha^2 \pi}{\alpha^2 \psi + q}} e^{-\frac{\alpha^2 \psi^2}{\alpha^2 \psi + q}} |1|^{-1}.$$

En substituant cette valeur et celles des deux autres intégrales de forme analogue, remplaçant ensuite la variable ψ par une autre s telle que $\psi = \frac{q}{s}$, différentiant par rapport à a , et observant qu'on a:

$$\left(\frac{1+\sqrt{-1}}{\sqrt{2}}\right)^3 = \sqrt{-1} e^{\frac{3}{4}\pi i},$$

on trouvera:

$$\frac{4a}{a^2} \frac{\sqrt{\pi}}{\Gamma(\frac{1}{2}(p-1))} \frac{e^{-\frac{1}{4}(p-2)\pi i}}{p-1} \int_0^\infty \frac{s^{1-\frac{1}{2}p} ds}{\sqrt{\left(1+\frac{s}{a^2}\right)^3 \left(1+\frac{s}{\beta^2}\right) \left(1+\frac{s}{\gamma^2}\right)}} \int_0^{+\infty} \frac{\sin q}{q^{2-\frac{1}{2}p}} e^{q\left(\frac{a^2}{a^2+s} + \frac{b^2}{\beta^2+s} + \frac{c^2}{\gamma^2+s}\right)\sqrt{-1}} dq.$$

Cette expression devant être réduite à sa partie réelle, tout revient à avoir celle de:

$$e^{-\frac{1}{4}(p-2)\pi i} \int_0^{+\infty} \frac{\sin q}{q^{2-\frac{1}{2}p}} e^{\sigma q \sqrt{-1}} dq,$$

en posant, pour abrégier:

$$\sigma = \frac{a^2}{a^2+s} + \frac{b^2}{\beta^2+s} + \frac{c^2}{\gamma^2+s}.$$

Or, cette intégrale en y remplaçant $\sin q$ par des exponentielles imaginaires, sera immédiatement donnée par l'équation (2), en ayant soin d'observer que le second membre de cette équation doit être remplacé par:

$$\frac{\Gamma(\rho) e^{-\frac{1}{2}\pi i}}{(-q)^\rho},$$

lorsque q a une valeur négative. On trouve ainsi que la partie réelle qu'il s'agit d'obtenir est zéro, ou:

$$-\frac{\Gamma(\frac{1}{2}p-1) \sin \frac{1}{2}p\pi}{2(1-\sigma)^{\frac{1}{2}p-1}} = \frac{\pi}{2\Gamma(2-\frac{1}{2}p)} \cdot \frac{1}{(1-\sigma)^{\frac{1}{2}p-1}},$$

suivant que $\sigma > 1$ ou $\sigma < 1$.

I. Si le point est intérieur, on aura:

$$\frac{a^2}{a^2} + \frac{b^2}{\beta^2} + \frac{c^2}{\gamma^2} < 1.$$

et par conséquent aussi $\sigma < 1$, la variable s étant positive. Il viendra donc:

$$A = \frac{2a\pi^{\frac{3}{2}}}{(p-1)a^2 \Gamma(\frac{1}{2}(p-1)) \Gamma(2-\frac{1}{2}p)} \int_0^{+\infty} \frac{s^{1-\frac{1}{2}p} ds}{\sqrt{\left(1+\frac{s}{a^2}\right)^3 \left(1+\frac{s}{\beta^2}\right) \left(1+\frac{s}{\gamma^2}\right)}} \left(1 - \frac{a^2}{a^2+s} - \frac{b^2}{\beta^2+s} - \frac{c^2}{\gamma^2+s}\right)^{1-\frac{1}{2}p}.$$

II. Si le point est extérieur, on déterminera la racine positive unique λ de l'équation $\sigma = 1$, et l'on aura évidemment $\sigma > 1$ ou $\sigma < 1$, suivant que $s < \lambda$ ou $s > \lambda$. L'expression de A sera donc, dans ce cas:

$$A = \frac{2a\pi^{\frac{3}{2}}}{(p-1)a^2 \Gamma(\frac{1}{2}(p-1)) \Gamma(2-\frac{1}{2}p)} \int_\lambda^{+\infty} \frac{s^{1-\frac{1}{2}p} ds}{\sqrt{\left(1+\frac{s}{a^2}\right)^3 \left(1+\frac{s}{\beta^2}\right) \left(1+\frac{s}{\gamma^2}\right)}} \left(1 - \frac{a^2}{a^2+s} - \frac{b^2}{\beta^2+s} - \frac{c^2}{\gamma^2+s}\right)^{1-\frac{1}{2}p}.$$

Si dans cette dernière expression on écrit $\lambda + s$ au lieu de s , et qu'on fasse:

$$a^2 + \lambda = a'^2, \quad a' = \frac{aa}{a'}, \quad \beta^2 + \lambda = \beta'^2, \quad b' = \frac{b\beta}{\beta'}, \quad \gamma^2 + \lambda = \gamma'^2, \quad c' = \frac{c\gamma}{\gamma'},$$

elle prendra la même forme que dans le cas du point intérieur, comme cela doit être en vertu du théorème des points correspondants, dû à M. IVORY, et qui, comme M. POISSON en a déjà fait la remarque, s'étend à toutes les lois d'attraction en fonction de la distance. Il est sans doute inutile d'ajouter que l'analyse que nous venons de développer, s'applique à toute intégrale dont la forme est semblable à celle de l'intégrale (1), et quel que soit le nombre des variables qu'elle puisse renfermer.

Comme second exemple j'indiquerai l'intégrale:

$$V = \int x^{p-1} y^{q-1} z^{r-1} \dots dx dy dz \dots,$$

qui doit être étendue à toutes les valeurs positives de x, y, z, \dots telles qu'on ait:

$$\left(\frac{x}{a}\right)^p + \left(\frac{y}{\beta}\right)^q + \left(\frac{z}{\gamma}\right)^r + \dots < 1,$$

les constantes $a, b, c, \dots p, q, r, \dots \alpha, \beta, \gamma, \dots$ étant également positives. Par une analyse toute semblable, on parvient à cette expression très simple, qu'on peut aussi obtenir par d'autres moyens, et qui renferme un grand nombre de résultats relatifs aux volumes, aux centres de gravité, moments d'inertie, etc.:

$$V = \frac{a^p \beta^q \gamma^r \dots}{pqr \dots} \frac{\Gamma\left(\frac{a}{p}\right) \Gamma\left(\frac{b}{q}\right) \Gamma\left(\frac{c}{r}\right) \dots}{\Gamma\left(1 + \frac{a}{p} + \frac{b}{q} + \frac{c}{r} + \dots\right)}.$$

En terminant, je ferai observer que l'intégrale transformée que l'on obtient au moyen du procédé indiqué, peut, dans beaucoup de cas, devenir indéterminée, à cause des limites infinies. Pour éviter les difficultés et même les inexactitudes que cette circonstance pourrait faire naître, on aura recours à l'artifice ingénieux dont MM. POISSON et CAUCHY ont fait usage dans différentes recherches, et qui consiste à remplacer l'intégrale proposée par une autre, dont la première puisse être considérée comme la limite, et qui reste complètement déterminée, lorsqu'on lui applique la méthode dont nous venons de donner quelques exemples.

ÜBER: EINE NEUE METHODE
ZUR BESTIMMUNG VIELFACHER INTEGRALE.

VON

G. LEJEUNE DIRICHLET.

ÜBER EINE NEUE METHODE ZUR BESTIMMUNG VIELFACHER INTEGRALE.

[Auszug aus einer in der Akademie der Wissenschaften

am 14. Februar 1839 gelesenen Abhandlung.]

Bekanntlich gehört die Bestimmung eines vielfachen Integrals oder auch die Zurückführung eines solchen auf ein anderes von einer niedrigeren Ordnung im Allgemeinen zu den schwierigeren Problemen, namentlich wenn die Integrationsgrenzen für die einzelnen Veränderlichen nicht constant sondern gegenseitig von einander abhängig sind, so dass der Umfang der Integrationen durch eine oder mehrere Ungleichheiten ausgedrückt ist, welche mehr als eine Veränderliche enthalten. Bei der Behandlung einiger physikalischen Aufgaben, welche schliesslich auf die Bestimmung einer Classe vielfacher Integrale von einer unbestimmten Ordnung zurückkommen, wurde der Verfasser auf die Methode geführt, welche den Gegenstand der Abhandlung bildet, und die nicht nur die Werthe der Integrale ergiebt, auf die es bei der genannten Untersuchung ankommt, sondern sich auch auf viele andere Integrale von den verschiedenartigsten Formen anwendbar erweist. Mit dieser Fruchtbarkeit vereinigt die Methode einen so hohen Grad von Einfachheit, dass man sich in der That wundern muss, dass dieselbe nicht schon früher auf ähnliche Untersuchungen angewendet worden ist. Das Princip dieser Art der Behandlung vielfacher Integrale, welche zwischen veränderlichen Grenzen zu nehmen sind, beruht auf der bekannten Eigenschaft gewisser bestimmter Integrale, die von den in ihnen enthaltenen Constanten in verschiedenen Intervallen auf verschiedene Weise abhängen, oder mit anderen Worten, welche discontinuirliche Functionen dieser

Constanten darstellen. So weiss man z. B., dass der einfache Ausdruck:

$$\frac{2}{\pi} \int_0^{\pi} \cos g \frac{\sin g}{g} dg$$

der Einheit gleich ist, so lange g zwischen -1 und $+1$ liegt, hingegen verschwindet, wenn g ausserhalb dieses Intervalles fällt. Hat man nun ein dreifaches Integral — und wir nehmen nur deshalb keines von einer höheren Ordnung, weil bei drei Veränderlichen dem Verfahren noch eine geometrische Deutung zukommt, welche den Gang desselben anschaulich anzusprechen erlaubt — welches über einen bestimmten Raum, z. B. über den von einer ellipsoidischen Fläche begrenzten zu erstrecken ist, so darf man nur bemerken, dass, wenn α, β, γ die halben Hauptaxen dieser Fläche bezeichnen, welche der Richtung nach mit den Coordinatenaxen zusammenfallen sollen, der Ausdruck:

$$\left(\frac{x}{\alpha}\right)^2 + \left(\frac{y}{\beta}\right)^2 + \left(\frac{z}{\gamma}\right)^2$$

unter oder über der Einheit liegt, je nachdem der Punkt (x, y, z) innerhalb oder ausserhalb des genannten Raumes liegt, um sogleich zu sehen, dass das bestimmte Integral:

$$\frac{2}{\pi} \int_0^{\pi} \frac{\sin g}{g} \cos \left(\left(\frac{x}{\alpha}\right)^2 + \left(\frac{y}{\beta}\right)^2 + \left(\frac{z}{\gamma}\right)^2 \right) g dg$$

innerhalb des Ellipsoids die Einheit zum Werthe hat, ausserhalb aber verschwindet. Multiplicirt man also den gegebenen Differentialausdruck $P dx dy dz$, wo P irgend eine Function von x, y, z bezeichnet, mit vorstehendem Integral, so hat man nun bei der Integration auf die ursprünglichen Grenzen keine Rücksicht mehr zu nehmen, d. h. man kann die Integrationen nach den Veränderlichen x, y, z zwischen den constanten Grenzen $-\infty$ und ∞ ausführen, indem offenbar durch den hinzugekommenen discontinuirlichen Factor die Elemente, auf welche sich die Integration nicht erstrecken soll, von selbst herausfallen. Man kann das eben angegebene Verfahren mit zwei Worten so charakterisiren, dass jedes über einen bestimmten Theil des Raumes, oder wenn man will, über eine nach allen Seiten hin begrenzte Masse auszudehnende Integral sogleich in ein anderes verwandelt werden kann, welches sich über den ganzen unendlichen Raum erstreckt und mithin in den meisten Fällen viel leichter zu behandeln sein wird, und zwar dadurch, dass man die Dichtigkeit ausserhalb des gege-

benen Umfanges der Null gleich werden lässt, welcher Voraussetzung immer leicht durch einen discontinuirlichen Factor genügt werden kann. Es ist überraschend, in welchem Grade durch diese Transformation, von welcher man auf den ersten Blick sich wenig Erfolg zu versprechen versucht ist, die schwierigsten Integrationen vereinfacht werden, und wie durch dieselbe Probleme, die auf anderem Wege sehr verborgene Kunstgriffe oder einen grossen Aufwand von Rechnung erfordern, ohne Schwierigkeit und mit alleiniger Hülfe einiger längst bekannter bestimmter Integrale gelöst werden können.

Von den in der Abhandlung gegebenen Anwendungen dieser Methode können hier nur einige der einfacheren kurz angedeutet werden. Als erstes Beispiel wählen wir die Attraction der Ellipsoide, welches Problem die Mathematiker so vielfach und mehr als irgend ein anderes der Integralrechnung beschäftigt hat.

Bekanntlich hat man bei diesem Probleme immer den Fall eines äusseren Punktes auf den des inneren, welcher weniger Schwierigkeiten darbietet, zurückgeführt, oder, wenn beide unabhängig von einander gelöst worden sind, so sind für jeden ganz verschiedene Mittel in Anwendung gekommen.

Durch das obige Verfahren werden beide Fälle einer ganz gleichförmigen und unabhängigen Behandlung fähig. Man hat erst dann einen Unterschied zwischen beiden zu machen, wenn man das Resultat der Untersuchung in seiner letzten und einfachsten Form aussprechen will. Ausserdem ist das Verfahren nicht auf die Voraussetzung beschränkt, dass die Attraction dem Quadrat der Entfernung umgekehrt proportional ist, sondern bleibt auch für jede andere ganze oder gebrochene Potenz der Entfernung anwendbar. Ebenso wenig braucht die Dichtigkeit der anziehenden Masse constant vorausgesetzt zu werden, sondern kann durch irgend eine rationale ganze Function der drei Coordinaten x, y, z ausgedrückt sein. Der Einfachheit wegen soll jedoch hier die Dichtigkeit als constant und der Einheit gleich angenommen werden.

Es seien α, β, γ die halben Axen des Ellipsoides, a, b, c die Coordinaten des angezogenen Punktes, x, y, z die irgend eines Punktes der anziehenden Masse. Es sei ferner:

$$\varrho^2 = (x-a)^2 + (y-b)^2 + (z-c)^2$$

und $\frac{1}{\varrho^p}$ das Attractionsgesetz, wo p zwischen 2 und 3 liegend angenommen wird, weil ausserhalb dieser Grenzen das Verfahren einige unbedeutende Mo-

dificationen erfordert. Nun ist bekanntlich die der Axe der x parallele Componente A der Attraction gleich dem nach a genommenen Differentialquotienten des über das ganze Ellipsoid zu erstreckenden Integrals:

$$-\frac{1}{p-1} \int \frac{dx dy dz}{q^{p-1}},$$

und nach dem oben Gesagten verwandelt sich dieses Integral in:

$$-\frac{2}{\pi(p-1)} \int_0^\infty \frac{\sin g}{g} dg \int \cos \left(\left(\frac{x}{a} \right)^2 + \left(\frac{y}{\beta} \right)^2 + \left(\frac{z}{\gamma} \right)^2 \right) g \frac{dx dy dz}{q^{p-1}},$$

wo jetzt die Integrationen nach x, y, z von $-\infty$ bis ∞ ausgedehnt werden können. Die Rechnung wird sehr vereinfacht, wenn man statt dieses Integrals das folgende betrachtet, dessen reeller Theil mit dem zu findenden zusammenfällt:

$$-\frac{2}{\pi(p-1)} \int_0^\infty \frac{\sin g}{g} dg \int e^{\left(\left(\frac{x}{a} \right)^2 + \left(\frac{y}{\beta} \right)^2 + \left(\frac{z}{\gamma} \right)^2 \right) g^2} q^{p-1} \frac{dx dy dz}{q^{p-1}},$$

Die Integrationen nach x, y, z lassen sich in dieser Form nicht bewerkstelligen; sie werden aber leicht ausführbar, wenn man den Factor $\frac{1}{q^{p-1}}$ mit Hülfe eines bestimmten Integrals so ausdrückt, dass die in q enthaltenen Coordinaten x, y, z , wie in dem andern Factor, nur im Exponenten vorkommen. Man kann sich zu diesem Zwecke der bekannten EULER'schen Formel bedienen:

$$(1) \quad \int_0^\infty e^{\psi^2} \psi^{r-1} d\psi = \frac{\Gamma(r)}{(\pm q)^r} e^{\pm \psi^2 \pi i - 1},$$

in welcher r positiv und < 1 sein muss, und die oberen oder die unteren Zeichen gelten, je nachdem q positiv oder negativ ist. Vermöge dieser Formel ist also:

$$\frac{1}{q^{p-1}} = \frac{1}{(q^2)^{\frac{1}{2}(p-1)}} = \frac{e^{-\frac{1}{2}(p-1)\pi i - 1}}{\Gamma(\frac{1}{2}(p-1))} \int_0^\infty e^{\psi^2} \psi^{\frac{1}{2}(p-3)} d\psi.$$

Substituirt man diesen Ausdruck, setzt für q^2 seinen Werth und berücksichtigt, dass:

$$\frac{1}{2}(p-1)\Gamma(\frac{1}{2}(p-1)) = \Gamma(\frac{1}{2}(p+1))$$

ist, so erhält man:

$$-\frac{1}{\pi \Gamma(\frac{1}{2}(p+1))} e^{\frac{1}{2}(1-p)\pi i - 1} \int_0^\infty \int_0^\infty \frac{\sin g}{g} \psi^{\frac{1}{2}(p-3)} e^{(a^2+b^2+c^2)\psi^2 - 1} U dg d\psi,$$

wo mit U zur Abkürzung das Product von drei nach x, y, z resp. genommenen einfachen Integralen bezeichnet ist, von denen das erste:

$$\int_{-\infty}^{\infty} e^{(\psi + \frac{g}{a^2})e^{2-2a\psi x}} V^{-1} dx$$

nach einer bekannten Formel, welche leicht aus (1) folgt, den Werth hat:

$$\sqrt{\frac{\pi}{2}} \frac{1+V^{-1}}{\sqrt{\psi + \frac{g}{a^2}}} e^{-\frac{a^2 a^2 \psi^2 V^{-1}}{a^2 \psi + g}}$$

Substituirt man diesen Ausdruck und die beiden anderen von gleicher Form und berücksichtigt, dass:

$$\left(\frac{1+V^{-1}}{\sqrt{2}}\right)^3 = V^{-1} e^{\frac{1}{2}\pi V^{-1}}$$

ist, so kommt:

$$-\frac{\sqrt{\pi} V^{-1}}{\Gamma(\frac{1}{2}(p+1))} e^{\frac{1}{2}(2-p)\pi V^{-1}} \int_0^\infty \int_0^\infty \frac{\psi^{p-3} \sin g}{g \sqrt{\left(\psi + \frac{g}{a^2}\right)\left(\psi + \frac{g}{\beta^2}\right)\left(\psi + \frac{g}{\gamma^2}\right)}} e^{g\psi\left(\frac{a^2}{g+a^2\psi} + \frac{b^2}{g+\beta^2\psi} + \frac{c^2}{g+\gamma^2\psi}\right)} V^{-1} dg d\psi.$$

Da die Ausdrücke im Exponenten und unter dem Wurzelzeichen homogene Functionen von g, ψ sind, so sieht man sogleich, dass sich das Integral vereinfachen wird, wenn man statt einer der Variablen g, ψ , etwa statt ψ , ihr Verhältniss zu der andern g einführt. Man setze also:

$$\psi = \frac{g}{s},$$

wo s die neue Veränderliche bezeichnet; dann werden die Grenzen für diese ∞ und 0 , und man kann dafür auch 0 und ∞ nehmen, wenn man dem ganzen Ausdruck das Minus-Zeichen vorsezt. Man erhält so, wenn man zur Abkürzung:

$$(2) \quad S = \frac{a^2}{a^2+s} + \frac{b^2}{\beta^2+s} + \frac{c^2}{\gamma^2+s}$$

setzt:

$$-\frac{\sqrt{\pi} V^{-1}}{\Gamma(\frac{1}{2}(p+1))} e^{\frac{1}{2}(2-p)\pi V^{-1}} \int_0^\infty \int_0^\infty \frac{g^{p-3} s^{1-\frac{1}{2}p} \sin g}{\sqrt{\left(1 + \frac{s}{a^2}\right)\left(1 + \frac{s}{\beta^2}\right)\left(1 + \frac{s}{\gamma^2}\right)}} e^{g s V^{-1}} dg ds.$$

Die Differentiation nach a ergibt den Ausdruck:

$$\frac{2a}{a^2} \frac{\sqrt{\pi}}{\Gamma(\frac{1}{2}(p+1))} e^{\frac{1}{2}(2-p)\pi V^{-1}} \int_0^\infty \frac{s^{1-\frac{1}{2}p}}{\sqrt{\left(1 + \frac{s}{a^2}\right)^3 \left(1 + \frac{s}{\beta^2}\right)\left(1 + \frac{s}{\gamma^2}\right)}} ds \int_0^\infty g^{\frac{1}{2}p-2} e^{g s V^{-1}} \sin g dg,$$

dessen reeller Theil nach Obigem die gesuchte Componente A darstellt. Um diesen reellen Theil zu erhalten, hat man nur den von:

$$\rho^{2(p-1)} \int_0^{\pi} q^{2p-2} \rho^{q^2-1} \sin q \, dq$$

zu suchen, welchen man sogleich findet, wenn man $\sin q$ durch Exponentialgrössen ausdrückt, und dann mit (1) vergleicht. Man gelangt so zu dem Resultat, dass der reelle Theil dieses Ausdrucks Null oder:

$$\frac{1}{2} \Gamma(\frac{1}{2}p-1) \sin(\frac{1}{2}p-1)\pi (1-S)^{1-\frac{1}{2}p} = \frac{\pi}{2 \Gamma(2-\frac{1}{2}p)} (1-S)^{1-\frac{1}{2}p}$$

ist, je nachdem $S > 1$ oder $S < 1$ ist.

Um nun das Endresultat hinzuschreiben, hat man zu unterscheiden, ob der angezogene Punkt (a, b, c) ein innerer oder äusserer ist.

I. Für einen inneren Punkt ist:

$$\frac{a^2}{\alpha^2} + \frac{b^2}{\beta^2} + \frac{c^2}{\gamma^2} < 1,$$

also auch:

$$S = \frac{a^2}{\alpha^2+s} + \frac{b^2}{\beta^2+s} + \frac{c^2}{\gamma^2+s} < 1,$$

da s positiv ist. Man erhält mithin:

$$A = \frac{a}{\alpha^2} \frac{\pi^{\frac{1}{2}}}{\Gamma(\frac{1}{2}(p+1)) \Gamma(2-\frac{1}{2}p)} \int_0^{\sigma} \frac{s^{1-\frac{1}{2}p}}{\left(1+\frac{s}{\alpha^2}\right)^3 \left(1+\frac{s}{\beta^2}\right) \left(1+\frac{s}{\gamma^2}\right)} (1-S)^{1-\frac{1}{2}p} ds,$$

II. Ist der Punkt ein äusserer, so hat man:

$$\frac{a^2}{\alpha^2} + \frac{b^2}{\beta^2} + \frac{c^2}{\gamma^2} > 1.$$

Der Ausdruck S ist also > 1 für $s = 0$. Da derselbe offenbar um so kleiner ist, je grösser s ist, und für $s = \infty$ verschwindet, so giebt es einen und nur einen positiven Werth σ von s , für welchen $S = 1$ ist. So lange $s < \sigma$ ist, wird offenbar $S > 1$; ist hingegen $s > \sigma$, so wird $S < 1$. Folglich hat man das Integral nach s nur von:

$$s = \sigma \quad \text{bis} \quad s = \infty$$

zu nehmen, und man erhält:

$$A = \frac{a}{\alpha^2} \frac{\pi^{\frac{1}{2}}}{\Gamma(\frac{1}{2}(p+1)) \Gamma(2-\frac{1}{2}p)} \int_{\sigma}^{\infty} \frac{s^{1-\frac{1}{2}p}}{\left(1+\frac{s}{\alpha^2}\right)^3 \left(1+\frac{s}{\beta^2}\right) \left(1+\frac{s}{\gamma^2}\right)} (1-S)^{1-\frac{1}{2}p} ds.$$

Für $p = 2$ fallen diese Resultate mit den bekannten für das NEWTON'sche Gesetz geltenden zusammen.

Ein anderes Beispiel der Anwendung unserer Methode bietet das Integral dar:

$$\int x^{a-1} y^{b-1} z^{c-1} \dots dx dy dz \dots,$$

welches über alle den Bedingungen:

$$x > 0, \quad y > 0, \quad z > 0, \quad \dots, \quad \left(\frac{x}{a}\right)^p + \left(\frac{y}{\beta}\right)^q + \left(\frac{z}{\gamma}\right)^r + \dots < 1,$$

genügenden Elemente auszudehnen ist, und wo $a, b, c, \dots, \alpha, \beta, \gamma, \dots, p, q, r, \dots$ positive Constanten bezeichnen. Durch eine ähnliche, jedoch weit einfachere Rechnung findet man für dieses Integral den Ausdruck:

$$\frac{\alpha^a \beta^b \gamma^c \dots}{p q r \dots} \frac{\Gamma\left(\frac{a}{p}\right) \Gamma\left(\frac{b}{q}\right) \Gamma\left(\frac{c}{r}\right) \dots}{\Gamma\left(1 + \frac{a}{p} + \frac{b}{q} + \frac{c}{r} + \dots\right)}.$$

Es ist einleuchtend, dass durch dieses Resultat die Bestimmung des körperlichen Inhaltes, des Schwerpunktes und des Trägheitsmomentes einer grossen Anzahl von Körpern auf einfache Quadraturen zurückgeführt ist.

Schliesslich ist noch zu bemerken, dass man dem oben beschriebenen Verfahren durch gewisse Modificationen eine grössere Ausdehnung geben oder die Anwendung desselben erleichtern kann. Eine dieser Modificationen, welche sich sehr leicht darbietet, und sich auf den Fall bezieht, wo der zu integrirende Ausdruck in Factoren zerfällt, besteht darin, einen derselben in den discontinuirlichen Factor hineinzuziehen.

Will man z. B. den Werth des Integrals:

$$\int \frac{dx dy dz \dots}{S^p T^q}$$

bestimmen, in welchem:

$$S = 1 + \left(\frac{x}{a}\right)^2 + \left(\frac{y}{b}\right)^2 + \dots, \quad T = 1 - \left(\frac{x}{\alpha}\right)^2 - \left(\frac{y}{\beta}\right)^2 - \dots$$

und die Integration über alle Elemente zu erstrecken ist, für welche T positiv

ist, so kann man leicht mit Hilfe der Gleichung (1) den Factor:

$$\frac{1}{T^q}$$

durch ein bestimmtes Integral ausdrücken, welches für ein negatives T verschwindet, so dass also hierdurch schon der Bedingung hinsichtlich der Begrenzung des Integrals genügt wird. Man findet so, dass das Integral (durch welches für den speciellen Fall zweier Variabeln x und y und der Werthe:

$$p = -\frac{1}{2}, \quad q = \frac{1}{2}$$

die Oberfläche des Ellipsoids bestimmt wird) immer auf Quadraturen zurückführbar ist.

ÜBER EINE NEUE METHODE
ZUR BESTIMMUNG VIELFACHER INTEGRALE.

VON

G. LEJEUNE DIRICHLET.

Abhandlungen der Königlich Preussischen Akademie der Wissenschaften von 1839, S. 61 — 79.

ÜBER EINE NEUE METHODE ZUR BESTIMMUNG VIELFACHER INTEGRALE.

[Vorgelesen in der Akademie der Wissenschaften am 14. Februar 1839.]

Bekanntlich gehört die Bestimmung eines vielfachen Integrals oder auch die Zurückführung eines solchen auf ein anderes von einer niedrigeren Ordnung im Allgemeinen zu den schwierigeren Problemen, namentlich wenn die Integrationsgrenzen für die einzelnen Veränderlichen nicht constant, sondern gegenseitig von einander abhängig sind, so dass der Umfang der Integrationen durch eine oder mehrere Ungleichheiten ausgedrückt ist, welche gleichzeitig mehrere der Veränderlichen enthalten. Bei der Behandlung einiger Aufgaben, welche schliesslich auf die Bestimmung einer Classe vielfacher Integrale von einer unbestimmten Ordnung zurückkommen, bin ich auf die Methode geführt worden, welche den Gegenstand dieser Abhandlung bildet, und die nicht nur die Werthe der Integrale ergiebt, auf welche es bei der genannten Untersuchung ankommt, sondern sich auch auf viele andere Integrale von den verschiedensten Formen anwendbar zeigt. Mit dieser Fruchtbarkeit verbindet die Methode einen so hohen Grad von Einfachheit, dass man sich in der That wundern muss, dass dieselbe nicht schon früher auf ähnliche Untersuchungen angewandt worden ist. Das Princip dieser Art der Behandlung vielfacher Integrale, bei welchen die einzelnen Integrationen nicht zwischen constanten Grenzen auszuführen sind, beruht auf der Möglichkeit discontinuirliche Functionen durch bestimmte Integrale auszudrücken. So weiss man zum Beispiel, dass der Ausdruck:

$$\frac{2}{\pi} \int_0^{\infty} \frac{\sin g}{g} \cos gg \, dg$$

der Einheit gleich ist, so lange die Constante g , abgesehen von ihrem Zeichen, unter der Einheit liegt, hingegen verschwindet, wenn die Constante die Einheit übersteigt. Hat man nun ein dreifaches Integral — und wir nehmen nur deshalb

nicht eines von beliebiger Ordnung, weil bei drei Variabeln dem Verfahren noch eine geometrische Deutung zukommt, welche das Wesen derselben anschaulich auszusprechen erlaubt — und soll dieses Integral über einen bestimmten Raum, z. B. über den von einer Ellipsoide begrenzten erstreckt werden, so darf man nur bemerken, dass, wenn α , β , γ die halben Hauptaxen der Grenzfläche bezeichnen und der Richtung nach mit den Coordinatenaxen zusammenfallen, der Ausdruck:

$$\left(\frac{x}{\alpha}\right)^2 + \left(\frac{y}{\beta}\right)^2 + \left(\frac{z}{\gamma}\right)^2$$

unter oder über der Einheit liegt, je nachdem der Punkt (x, y, z) im inneren oder im äusseren Raume sich befindet, um sogleich zu sehen, dass das Integral:

$$\frac{2}{\pi} \int_0^{\pi} \frac{\sin g}{g} \cos \left[\left(\frac{x}{\alpha}\right)^2 + \left(\frac{y}{\beta}\right)^2 + \left(\frac{z}{\gamma}\right)^2 \right] g dg$$

im Inneren die Einheit zum Werthe hat ausserhalb aber verschwindet. Multipliziert man also den gegebenen Differentialausdruck:

$$P dx dy dz,$$

wo P irgend eine Function von x , y , z bezeichnet, mit vorstehendem Integral, so hat man bei der Integration auf die ursprünglichen Grenzen keine Rücksicht mehr zu nehmen, d. h. man kann die Integrationen in Bezug auf x , y , z zwischen den Grenzen $-\infty$ und ∞ ausführen, indem offenbar durch den hinzutretenden discontinuirlichen Factor die Elemente, auf welche sich die Integration nicht erstrecken soll, von selbst herans fallen. Um das eben beschriebene Verfahren mit zwei Worten zu charakterisiren, kann man sagen, dass jedes über einen bestimmten Theil des unendlichen Raumes oder, wenn man will, über eine nach allen Seiten hin begrenzte Masse auszudehnende Integral sogleich in ein anderes verwandelt werden kann, welches sich über den ganzen unendlichen Raum erstreckt und mithin in den meisten Fällen leichter zu behandeln sein wird, und zwar dadurch, dass man die Dichtigkeit im äusseren Raume verschwinden lässt, welcher Forderung immer leicht durch einen discontinuirlichen Factor genügt werden kann. Es ist überraschend, in welchem Grade durch diese Umformung, von der man auf den ersten Blick sich wenig Erfolg zu versprechen versucht ist, die schwierigsten Integrationen vereinfacht werden, und wie durch dieselbe Probleme, die auf anderen Wegen verborgene Kunstgriffe oder einen grossen Aufwand von Rechnung erfordern, ohne Schwierigkeit

und mit alleiniger Hülfe einiger bestimmter Integrale gelöst werden können, welche wegen ihrer Wichtigkeit und ihres häufigen Vorkommens längst in die Elementarwerke übergegangen sind.

§. 1.

Ehe wir dazu übergehen, die in der Einleitung beschriebene Methode zur Bestimmung oder Reduction vielfacher Integrale auf Beispiele anzuwenden, wird es zweckmässig sein, einige allgemeine Bemerkungen über gewisse Schwierigkeiten voranzuschicken, welche diese Anwendung zuweilen darbieten kann. Ist:

$$\int P dx dy \dots$$

ein vielfaches Integral, in welchem P eine beliebige Function der Variabeln x, y, \dots darstellt und dessen Umfang wir uns durch Ungleichheitsbedingungen zwischen diesen oder auf irgend eine andere Weise bestimmt denken, so können zwei wesentlich verschiedene Fälle eintreten, welche denen ganz ähnlich sind, die bei unendlichen Reihen statt finden. Setzt man nämlich an die Stelle der Function ihren numerischen oder absoluten Werth, so wird das so modifizierte, in demselben Umfange genommen gedachte Integral entweder einen endlichen Werth erhalten oder unendlich gross werden. Im ersteren Falle hat das ursprüngliche Integral einen völlig bestimmten endlichen Werth, welcher von der Ordnung, worin die Integrationen ausgeführt werden, ganz unabhängig ist und auch derselbe bleibt, wenn man statt der Veränderlichen x, y, \dots irgend welche neue einführt^{*)}. Ganz anders verhält sich die Sache im zweiten der eben erwähnten Fälle: das Integral ist dann wesentlich unbestimmt oder unendlich. Nimmt dasselbe bei einer gewissen Aufeinanderfolge der einzelnen Integrationen einen bestimmten endlichen Werth an, so kann bei veränderter Ordnung derselben oder nach Einführung neuer Variabeln ein solcher zu existiren aufhören, oder, wenn dies auch nicht der Fall sein sollte, so kann dieser Werth von demjenigen verschieden sein, welcher der Art, wie die Integrationen zuerst ausge-

^{*)} Es ist hier nur von der Einführung neuer Variabeln im gewöhnlichen Sinne des Wortes die Rede, bei welcher Operation an die Stelle der ursprünglichen Variabeln x, y, \dots andere p, q, \dots in gleicher Anzahl treten, welche bestimmte Functionen der ersteren sind. Zerlegt man hingegen jedes Element des gegebenen Integrals durch Einführung neuer Integrale in unendlich viele neue Elemente, so kann das so entstehende Integral einer höheren Ordnung natürlich unbestimmt werden, obgleich das ursprüngliche einen völlig bestimmten endlichen Werth hatte. Es kommt dabei lediglich darauf an, ob die in das gegebene Integral eingeführten neuen Integrale völlig bestimmte sind oder nicht.

führt wurden, entsprach. Es folgt daraus, dass, wenn ein Integral der zweiten Art, bei einer bestimmten Ordnung der Integrationen, Gegenstand der Untersuchung ist, man keine der oben genannten Veränderungen damit vornehmen kann, ohne sich vorher überzeugt zu haben, dass diese keinen Einfluss auf das Resultat ausübt. Gewöhnlich wird man diesen Zweck dadurch erreichen, dass man statt der Function P eine andere allgemeinere P_ε einführt, welche eine neue Constante ε enthält und für $\varepsilon = 0$ in P übergeht. Ist alsdann das Integral $\int P_\varepsilon dx dy \dots$ zwischen denselben Grenzen und, so lange als ε von Null verschieden ist, ein völlig bestimmtes, und lässt sich zugleich nachweisen, dass der Unterschied zwischen den Integralen:

$$\int P dx dy \dots \quad \int P_\varepsilon dx dy \dots$$

vor und nach der beabsichtigten Veränderung für ein unendlich kleines ε selbst unendlich klein wird, so kann man daraus schliessen, dass auch das Integral $\int P dx dy \dots$ von dieser Veränderung nicht afficirt wird. Es ist dieses Verfahren demjenigen ganz analog, welches mehrere Mathematiker und namentlich POISSON und CAUCHY schon angewandt haben, um ähnlichen Unbestimmtheiten vorzubeugen. Über die Wahl der Function P_ε lassen sich keine allgemeinen Vorschriften geben. In bestimmten Fällen wird man jedoch in dieser Beziehung nur höchst selten auf erhebliche Schwierigkeiten stossen: vielmehr wird man bei einiger Übung leicht dahin gelangen, ohne das im Vorhergehenden ange deutete Verfahren wirklich anzuwenden, aus der blossen Ansicht der gegebenen Function P zu erkennen, ob das zu behandelnde Integral die beabsichtigte Umformung zulässt oder nicht.

§. 2.

Als erstes Beispiel der Anwendung der oben beschriebenen Methode wählen wir das Integral:

$$(1) \quad \int \dots \int \dots e^{-ax} x^{k-1} e^{-by} y^{b-1} dx dy \dots$$

in welchem k, a, b, \dots positive Constanten bezeichnen, und welches über alle positiven Werthe der Veränderlichen ausgedehnt werden soll, die der Bedingung:

$$(2) \quad \sigma = x + y + \dots < 1$$

genügen. Es wird, wie immer in ähnlichen Fällen, vorausgesetzt, dass die In-

emente dx, dy, \dots positiv sein sollen. Multiplicirt man das Element dieses vielfachen Integrals mit:

$$\frac{2}{\pi} \int_0^{\infty} \frac{\sin g}{g} \cos \sigma g \, dg,$$

so wird man nach der oben bemerkten Eigenschaft dieses Ausdrucks die Integrationen nach den einzelnen Variablen x, y, \dots zwischen den Grenzen 0 und ∞ ausführen dürfen. Man erhält so:

$$(3) \quad \frac{2}{\pi} \iiint \dots e^{-\lambda a} x^{a-1} dx, y^{b-1} dy \dots \frac{\sin g}{g} \cos \sigma g \, dg.$$

Dieses neue Integral ist kein völlig bestimmtes, und es bedarf einer Untersuchung, ob dasselbe seinen Werth nicht ändert, wenn wir, statt erst nach g und dann nach x, y, \dots zu integriren, wie es eigentlich geschehen sollte, was uns aber zu dem Integral (1) zurückführen würde, die Integrationen nach x, y, \dots der nach g vorangehen lassen. Um sich in diesem Falle zu überzeugen, dass die so veränderte Ordnung der Operationen keinen Einfluss auf das Resultat ausübt, darf man nur unter den Zeichen mit $e^{-\varepsilon g}$ multipliciren. So lange die positive Constante ε von Null verschieden ist, bleibt das so modificirte Integral völlig bestimmt, und man sieht sogleich, dass der Werth desselben für ein unendlich klein werdendes ε das Integral (3) zur Grenze hat, man mag in diesem mit der Integration nach g oder mit denen nach x, y, \dots beginnen. Wir dürfen daher in dem Integral (3) zuerst nach x, y, \dots integriren. Wir sehen so, und wenn wir zugleich statt $\cos \sigma g$ die imaginäre Exponentialgrösse $e^{-\sigma g i}$, wo i wie gewöhnlich $\sqrt{-1}$ bedeutet, einführen, dass das Integral (3) mit dem reellen Theile des folgenden zusammenfällt:

$$\frac{2}{\pi} \int_0^{\infty} \frac{\sin g}{g} Q \, dg,$$

wo Q zur Abkürzung ein Product von einfachen, nach x, y, \dots zu nehmenden Integralen bezeichnet, von welchen das auf x sich beziehende die Form hat:

$$\int_0^{\infty} e^{-(k+g i)x} x^{a-1} dx,$$

und nach einer bekannten, zuerst von EULER durch Induction gefundenen Formel dem Ausdruck:

$$\frac{\Gamma(a)}{(k+g i)^a}.$$

gleich ist, in welchem die im Allgemeinen vieldentige Potenz, wie ebenfalls bekannt ist, durch die Gleichung:

$$(k+gi)^a = (k^2+g^2)^{\frac{1}{2}a} e^{\operatorname{arctg} \frac{g}{k}}$$

zu bestimmen ist, worin arctg innerhalb des Intervalls zwischen $-\frac{1}{2}\pi$ und $\frac{1}{2}\pi$ genommen werden muss.

Durch Substitution dieses Werthes und der Werthe von ähnlicher Form für die übrigen Integrale erhalten wir:

$$\frac{2}{\pi} \Gamma(a)\Gamma(b)\dots \int_0^{\infty} \frac{\sin g}{g} \frac{1}{(k+gi)^{a+b+\dots}} dg,$$

so dass also das vorgelegte vielfache Integral (1) auf den reellen Theil dieses einfachen zurückgeführt ist. Man kann diesem letzteren eine andere Form geben. Wenn nämlich in dem eben erhaltenen, für beliebig viele Veränderliche x, y, \dots gültigen Resultat nur eine Veränderliche x als vorhanden angenommen und zugleich die Constante a in $a+b+\dots$ verwandelt wird, so zeigt sich, dass das Integral:

$$\int_0^1 e^{-kx} x^{a+b+\dots-1} dx$$

gleich dem reellen Theile des Ausdrucks:

$$\frac{2}{\pi} \Gamma(a+b+\dots) \int_0^{\infty} \frac{\sin g}{g} \frac{1}{(k+gi)^{a+b+\dots}} dg$$

ist. Führt man daher statt dieses reellen Theiles das Integral $\int_0^1 e^{-kx} x^{a+b+\dots-1} dx$ in das allgemeine Resultat ein, so kommt:

$$\iint \dots e^{-k(x+y+\dots)} x^{a-1} dx y^{b-1} dy \dots = \frac{\Gamma(a)\Gamma(b)\dots}{\Gamma(a+b+\dots)} \int_0^1 e^{-kx} x^{a+b+\dots-1} dx,$$

wo das vielfache Integral sich über alle positiven der Bedingung (2) genügenden Werthe erstreckt. Man sieht sogleich, dass diese Gleichung ihre Gültigkeit nicht verliert, wenn man die bisher positiv vorausgesetzte Constante k in Null übergehen lässt, und erhält so:

$$\iint \dots x^{a-1} dx y^{b-1} dy \dots = \frac{\Gamma(a)\Gamma(b)\dots}{(a+b+\dots)\Gamma(a+b+\dots)} = \frac{\Gamma(a)\Gamma(b)\dots}{\Gamma(1+a+b+\dots)}.$$

Für den Fall, wo nur zwei Variablen vorhanden sind, geht die eben erhaltene Gleichung in diejenige über, durch welche die EULER'schen Integrale der ersten Gattung auf die der zweiten zurückgeführt werden,

Man kann in die allgemeine Gleichung eine grössere Anzahl von Constanten einführen, indem man statt x, y, \dots beziehungsweise:

$$\left(\frac{x}{\alpha}\right)^p, \left(\frac{y}{\beta}\right)^q, \dots$$

setzt, wo $\alpha, \beta, \dots, p, q, \dots$ neue positive Constanten bezeichnen. Das vielfache Integral wird so:

$$\frac{p}{\alpha} \frac{q}{\beta} \dots \iint \dots \left(\frac{x}{\alpha}\right)^{ap-1} dx \cdot \left(\frac{y}{\beta}\right)^{bq-1} dy \dots$$

mit der Grenzbedingung:

$$\left(\frac{x}{\alpha}\right)^p + \left(\frac{y}{\beta}\right)^q + \dots < 1.$$

Schreibt man zugleich $\frac{a}{p}, \frac{b}{q}, \dots$ statt a, b, \dots , so geht die Gleichung in die folgende über:

$$\iint \dots x^{a-1} dx \cdot y^{b-1} dy \dots = \frac{\alpha^a \beta^b \dots}{p q \dots} \frac{\Gamma\left(\frac{a}{p}\right) \Gamma\left(\frac{b}{q}\right) \dots}{\Gamma\left(1 + \frac{a}{p} + \frac{b}{q} + \dots\right)}.$$

wo der Umfang der Integrationen durch die vorher aufgestellte Ungleichheit bestimmt wird.

Es ist einleuchtend, dass durch dieses Resultat, auf drei Variabeln beschränkt, die Bestimmung des Inhaltes, des Schwerpunktes und des Trägheitsmomentes für eine grosse Anzahl von Körpern auf die EULER'schen Integrale zurückgeführt wird. So sieht man z. B., wenn man $a = b = c = 1$ setzt, dass durch:

$$\frac{\alpha \beta \gamma}{p q r} \frac{\Gamma\left(\frac{1}{p}\right) \Gamma\left(\frac{1}{q}\right) \Gamma\left(\frac{1}{r}\right)}{\Gamma\left(1 + \frac{1}{p} + \frac{1}{q} + \frac{1}{r}\right)}$$

der Raum ausgedrückt ist, welcher von den zwischen den positiven Coordinatenaxen liegenden Theilen der Coordinatenebenen und der Fläche:

$$\left(\frac{x}{\alpha}\right)^p + \left(\frac{y}{\beta}\right)^q + \left(\frac{z}{\gamma}\right)^r = 1,$$

begrenzt wird. Sind p, q, r gerade Zahlen oder Brüche, die in ihrer ein-

fachsten Gestalt grade Zahlen zu Zählern haben, so wird der bloss von der Fläche eingeschlossene Raum das Achtefache des eben gefundenen Ausdrucks sein.

Es ist also namentlich der von der Fläche:

$$\left(\frac{x}{\alpha}\right)^4 + \left(\frac{y}{\beta}\right)^4 + \left(\frac{z}{\gamma}\right)^4 = 1$$

eingeschlossene Raum:

$$\frac{1}{8} \alpha \beta \gamma \frac{\Gamma(\frac{1}{4})^3}{\Gamma(\frac{3}{4})},$$

und hängt nach den bekannten Eigenschaften der Function Γ bloss von dem Integral $\int_0^1 \frac{dx}{\sqrt{1-x^4}}$ ab, welches die Länge der Lemniscate ausdrückt.

§. 3.

In dem eben behandelten Falle liessen sich nach Einführung des discontinuirlichen Factors und durch eine blosse Umkehrung der Integrationsordnung die Integrationen nach den ursprünglichen Veränderlichen ohne Schwierigkeit ausführen. Bei anderen Formen des gegebenen Integrals kann es erforderlich werden, noch andere Umformungen mit demselben vorzunehmen, um dasselbe auf die niedrigste Ordnung, deren es fähig ist, zurückzuführen. Zu den wirksamsten Transformationen dieser Art gehört, nebst der Einführung neuer Variablen, die Zerlegung des zu integrierenden Elementes in eine unendliche Anzahl neuer Elemente einer höheren Ordnung, oder was dasselbe ist, die Einführung neuer Integralzeichen unter den schon vorhandenen. Nimmt man zu dieser Umformung seine Zuflucht, so wird es fast immer vorthellhaft sein, dieselbe mit der Einführung des Discontinuitätsfactors zu einer Operation zu verschmelzen, indem man die neu aufzunehmenden Integrale so wählt, dass sie den Grenzbedingungen schon von selbst genügen und also den discontinuirlichen Factor ganz überflüssig machen. Enthält z. B. das Element des ursprünglichen Integrals den Factor $\frac{1}{\sigma^q}$, wo q eine positive, die Einheit nicht übersteigende Constante, und σ irgend eine Function der Veränderlichen bezeichnet, und sollen alle nach diesen zu bewerkstelligenden Integrationen sich nur auf solche Werthe derselben erstrecken, denen ein positives σ entspricht, so kann man leicht den Factor $\frac{1}{\sigma^q}$ durch ein bestimmtes Integral darstellen, welches diesen nur für ein positives σ ausdrückt, für ein negatives dagegen verschwindet.

Zu diesem Zweck kann die Gleichung:

$$\int_0^{\infty} e^{\sigma\psi} \psi^{q-1} d\psi = \frac{\Gamma(q)}{(\pm\sigma)^q} e^{\pm\frac{1}{2}q\pi}$$

diene, welche ein specieller Fall der schon im vorigen Paragraphen gebrauchten ist, und worin die oberen oder die unteren Zeichen gelten, je nachdem σ positiv oder negativ ist. Sie zerfällt in die beiden folgenden:

$$\int_0^{\infty} \cos\sigma\psi \psi^{q-1} d\psi = \frac{\Gamma(q)\cos\frac{1}{2}q\pi}{(\pm\sigma)^q}, \quad \int_0^{\infty} \sin\sigma\psi \psi^{q-1} d\psi = \pm \frac{\Gamma(q)\sin\frac{1}{2}q\pi}{(\pm\sigma)^q}.$$

Multipliziert man diese resp. mit $\sin\frac{1}{2}q\pi$ und $\cos\frac{1}{2}q\pi$ und addirt, so erhält man:

$$\int_0^{\infty} \sin(\frac{1}{2}q\pi + \sigma\psi) \psi^{q-1} d\psi = \frac{\Gamma(q)\sin\frac{1}{2}(q\pi \pm q\pi)}{(\pm\sigma)^q},$$

so dass also:

$$\frac{1}{\Gamma(q)\sin q\pi} \int_0^{\infty} \sin(\frac{1}{2}q\pi + \sigma\psi) \psi^{q-1} d\psi = \frac{1}{\sigma^q} \quad \text{oder} \quad = 0$$

wird, je nachdem σ positiv oder negativ ist.

Mit Hilfe dieser Formel lässt sich z. B. das Integral:

$$U = \iiint \dots \frac{1}{(\lambda + \alpha x + \beta y + \dots)^p} \frac{1}{(1 - x - y - \dots)^q} x^{\alpha-1} dx \cdot y^{\beta-1} dy \dots \quad (x+y+\dots < 1)$$

so wie das Integral:

$$V = \iint \dots \frac{1}{(\lambda + \alpha x + \beta y + \dots)^p} \frac{1}{(-1 + x + y + \dots)^q} x^{\alpha-1} dx \cdot y^{\beta-1} dy \dots \quad (x+y+\dots > 1)$$

auf einfache Quadraturen zurückzuführen.

Um dies mit der grössten Kürze zu thun, wollen wir ein etwas allgemeineres betrachten, welches beide in sich begreift.

§. 4.

Setzt man zur Abkürzung:

$$\lambda + \alpha x + \beta y + \dots = \rho, \quad 1 - x - y - \dots = \sigma,$$

wobei $\lambda, \alpha, \beta, \dots$ positive Constanten bezeichnen, und sind $\varepsilon, p, q, a, b, \dots$ ebenfalls positive Constanten, welche der Bedingung:

$$p + q > a + b + \dots$$

genügen, so ist, wie leicht zu sehen, das vielfache Integral:

$$W = \int \int \dots \frac{1}{\rho^p} \frac{1}{(\varepsilon + \sigma i)^q} x^{\alpha-1} dx \cdot y^{\beta-1} dy \dots,$$

welches sich über alle positiven Werthe der Variablen erstrecken soll, und worin die Potenz mit imaginärer Basis in demselben Sinne, wie in §. 2, genommen gedacht wird, ein völlig bestimmtes.

Da ρ und ε positiv sind, so hat man:

$$\int_0^{\infty} e^{-\rho q} q^{p-1} dq = \frac{\Gamma(p)}{\rho^p} \cdot \int_0^{\infty} e^{-(\varepsilon + \sigma i)\psi} \psi^{q-1} d\psi = \frac{\Gamma(q)}{(\varepsilon + \sigma i)^q}.$$

Nach der oben gemachten Bemerkung wird das Integral nach Einsetzung dieser Werthe nicht aufhören völlig bestimmt zu sein. Man kann daher die Integrationen nach x , y , ... als die zuerst auszuführenden betrachten und hat dann:

$$W = \frac{1}{\Gamma(p)\Gamma(q)} \int_0^{\infty} \int_0^{\infty} e^{-\lambda q - (\varepsilon + \sigma i)\psi} q^{p-1} \psi^{q-1} Q dq d\psi,$$

wo Q ein Product von einfachen Integralen bedeutet, von denen das nach x zu nehmende:

$$\int_0^{\infty} e^{-(\alpha q - \psi)x} x^{p-1} dx = \frac{\Gamma(p)}{(\alpha q - \psi)^p}$$

ist.

Durch Substitution dieses Ausdruckes und der übrigen von ähnlicher Form erhält man:

$$W = \frac{\Gamma(a)\Gamma(b)\dots}{\Gamma(p)\Gamma(q)} \int_0^{\infty} \int_0^{\infty} e^{-\lambda q - (\varepsilon + \sigma i)\psi} q^{p-1} \psi^{q-1} \frac{1}{(\alpha q - \psi)^p} \frac{1}{(\beta q - \psi)^q} \dots dq d\psi.$$

Bei aufmerksamer Betrachtung dieses Doppelintegrals sieht man sogleich, dass sich eine der beiden Integrationen wird ausführen lassen, wenn man statt einer der beiden Variablen, z. B. statt ψ , ihr Verhältniss zur andern als neue Veränderliche einführt. Setzt man also $\psi = q s$, $d\psi = q ds$ und integrirt dann nach q , so kommt:

$$W = \frac{\Gamma(m)\Gamma(a)\Gamma(b)\dots}{\Gamma(p)\Gamma(q)} \int_0^{\infty} \frac{s^{q-1}}{(\lambda + (\varepsilon + \sigma i)s)^m} \frac{1}{(\alpha - s)^p} \frac{1}{(\beta - s)^q} \dots ds.$$

wo m zur Abkürzung für $p+q-a-b-\dots$ gesetzt worden ist.

Durch diese Gleichung ist also das vielfache Integral W auf ein einfaches zurückgeführt. Da das Resultat für jeden positiven Werth von ε gilt,

so dürfen wir ε als unendlich klein ansehen. Fügen wir aber zu den schon gemachten Voraussetzungen über die Constanten noch die hinzu, dass der Werth von q ein ächter Bruch sei, so wird sowohl die erste als die zweite Seite der Gleichung für ein unendlich klein werdendes ε nur unendlich wenig von dem Werthe, der $\varepsilon = 0$ entspricht, verschieden sein und folglich die Gleichung für $\varepsilon = 0$ noch gelten. Für das Integral auf der rechten Seite ist dies einleuchtend, und man wird sich auch hinsichtlich des vielfachen Integrals leicht von der Richtigkeit dieser Behauptung überzeugen, wenn man dieses in drei andere W_1, W_2, W_3 zerlegt, welche sich resp. über die Werthe der Veränderlichen erstrecken, welche den Bedingungen:

$$\sigma > k, \quad -k < \sigma < k, \quad \sigma < -k$$

genügen, in denen k einen constanten positiven Bruch bezeichnet. Offenbar haben dann die Integrale W_1 und W_3 für ein ins Unendliche abnehmendes ε die Integrale von ähnlicher Form, in denen geradezu $\varepsilon = 0$ gesetzt ist, zu Grenzen, und was das zweite W_2 betrifft, so sieht man eben so leicht, dass dieses oder vielmehr der reelle Theil, so wie der Coefficient des imaginären Theiles desselben, sowohl für $\varepsilon = 0$, als für ein unendlich kleines ε , unter einer gewissen Grenze liegt, welche beliebig klein ausfällt, wenn die Constante k gehörig klein gedacht wird, woraus dann die aufgestellte Behauptung sogleich folgt.

Berücksichtigen wir nun, dass der Ausdruck:

$$\frac{1}{(\varepsilon + \sigma i)^q}$$

nach der Bedeutung, worin derselbe hier zu nehmen ist, für $\varepsilon = 0$ in:

$$\frac{1}{\sigma^q} e^{-\frac{1}{2}q\pi i} \quad \text{oder in} \quad \frac{1}{(-\sigma)^q} e^{\frac{1}{2}q\pi i}$$

übergeht, je nachdem σ positiv oder negativ ist, so sehen wir, dass das Element des vielfachen Integrals nach diesen beiden Fällen eine verschiedene Form annimmt, und dass also das Integral W von selbst in zwei andere zerfällt. Wir erhalten so die Gleichung:

$$e^{-\frac{1}{2}q\pi i} U + e^{\frac{1}{2}q\pi i} V = \frac{\Gamma(m)\Gamma(a)\Gamma(b)\dots}{\Gamma(p)\Gamma(q)} \int_0^\infty \frac{s^{q-1} ds}{(\lambda + si)^m (\alpha - si)^a (\beta - si)^b \dots},$$

in welcher U und V dieselben Integrale und zwischen denselben Grenzen, wie im vorigen Paragraphen, bedeuten. Diese Gleichung giebt, da sie die imaginäre

Grösse i enthält, sogleich zwei andere, welche zur Bestimmung der beiden Integrale U und V dienen. Durch Differentiation oder Integration nach den in diesen Gleichungen enthaltenen Constanten lassen sich die Werthe von anderen vielfachen Integralen ableiten, die theils von U und V der Form nach verschieden, theils mit diesen in der Form übereinstimmend, von einigen der Beschränkungen, denen die Constanten in U und V unterworfen waren, befreit sind. Wir übergangen jedoch diese Folgerungen, da wir nur den Zweck haben, die Anwendung der oben beschriebenen Methode an einigen Beispielen zu zeigen.

§. 5.

Zum Schlusse wollen wir die Attraction eines homogenen Ellipsoides bestimmen, welches Problem bekanntlich die Mathematiker mehr als irgend ein anderes der Integralrechnung beschäftigt hat.

Es seien α, β, γ die halben Axen des Ellipsoides, a, b, c die Coordinaten des angezogenen Punctes, x, y, z die irgend eines Punctes der anziehenden Masse. Es sei ferner:

$$\varrho^2 = (x-a)^2 + (y-b)^2 + (z-c)^2,$$

und $\frac{1}{\varrho^p}$ das Attractionsgesetz, wo p zwischen 2 und 3 angenommen wird, weil ausserhalb dieser Grenzen das Verfahren einige unbedeutende Modificationen erfordert. Dann ist bekanntlich die mit der Axe der x parallele und nach der Seite, nach welcher die x abnehmen, als positiv zu betrachtende Componente A der Attraction gleich dem nach a genommenen partiellen Differentialquotienten des über den ganzen ellipsoidischen Körper auszudehnenden dreifachen Integrals:

$$(1) \quad -\frac{1}{p-1} \int \frac{dx dy dz}{\varrho^{p-1}}.$$

Nach dem oben Bemerkten verwandelt sich dieses Integral in das folgende:

$$-\frac{2}{\pi(p-1)} \int_0^\pi \frac{\sin \varphi}{\varphi} d\varphi \int \cos \left(\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} + \frac{z^2}{\gamma^2} \right) \varphi \frac{dx dy dz}{\varrho^{p-1}},$$

wosich jetzt die Integrationen nach x, y, z von $-\infty$ bis ∞ erstrecken dürfen. Die Rechnung wird sehr vereinfacht, wenn man statt des vorhergehenden Integrals das folgende betrachtet, dessen reeller Theil mit jenem zusammenfällt:

$$-\frac{2}{\pi(p-1)} \int_0^\pi \frac{\sin \varphi}{\varphi} d\varphi \int e^{\left(\frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} + \frac{z^2}{\gamma^2} \right) \varphi i} \frac{dx dy dz}{\varrho^{p-1}}.$$

Die Integrationen nach x, y, z lassen sich in dieser Form nicht bewerkstelligen; sie werden aber leicht ausführbar, wenn man den Factor $\frac{1}{\rho^{p-1}}$ mittelst der schon in §. 3 angeführten Gleichung durch ein bestimmtes Integral ausdrückt. Da ρ^2 positiv ist, so hat man:

$$\int_0^{\infty} e^{\rho^2 \psi^2} \psi^{p(p-3)} d\psi = \frac{\Gamma(\frac{1}{2}(p-1))}{\rho^{p-1}} e^{\frac{1}{2} p(p-1)\pi i}.$$

Durch Substitution dieses Werthes und mit Berücksichtigung, dass:

$$\frac{1}{2}(p-1)\Gamma(\frac{1}{2}(p-1)) = \Gamma(\frac{1}{2}(p+1))$$

ist, erhält man:

$$(2) \quad - \frac{1}{\pi \Gamma(\frac{1}{2}(p+1))} e^{\frac{1}{2}(1-p)\pi i} \int_0^{\infty} \int_0^{\infty} \frac{\sin g}{g} \psi^{p(p-3)} e^{i(\alpha^2 + \beta^2 + \gamma^2)\psi^2} Q d\psi,$$

wobei Q ein Product von drei nach x, y, z resp. genommenen einfachen Integralen bezeichnet, wovon das erste:

$$\int_{-\infty}^{\infty} e^{\left(\psi + \frac{g}{a^2}\right)^2 i - 2\alpha\psi x i} dx,$$

den Ausdruck:

$$\frac{e^{\frac{1}{2}\pi i} \sqrt{\pi}}{\sqrt{\psi + \frac{g}{a^2}}} e^{-\frac{a^2 \alpha^2 \psi^2 i}{g + a^2 \psi}}$$

zum Werthe hat, wie dies aus einer bekannten Formel folgt. In der That hat man:

$$\int_{-\infty}^{\infty} e^{i(lx^2 + 2mx)} dx = \sqrt{\frac{\pi}{l}} e^{\frac{\pi}{4} i} e^{-\frac{m^2 i}{l}},$$

wenn l , wie es hier der Fall ist, positiv ist. Diese Gleichung ist eine sehr einfache Folgerung aus der schon angeführten des §. 3. und daraus, dass $\Gamma(\frac{1}{2}) = \sqrt{\pi}$ ist.

Substituirt man diesen Ausdruck und die beiden anderen von ganz gleicher Form, und setzt zugleich $i e^{\frac{1}{2}\pi i}$ statt $e^{\frac{3}{2}\pi i}$, so erhält man:

$$(3) \quad - \frac{i \sqrt{\pi}}{\Gamma(\frac{1}{2}(p+1))} e^{(2-p)\frac{\pi}{4} i} \int_0^{\infty} \int_0^{\infty} \frac{\sin g}{g} \psi^{p(p-3)} \frac{e^{8g^2 i}}{\sqrt{\left(\psi + \frac{g}{\alpha^2}\right) \left(\psi + \frac{g}{\beta^2}\right) \left(\psi + \frac{g}{\gamma^2}\right)}} d\psi d\psi,$$

wo zur Abkürzung:

$$S = \left(\frac{a^2}{g+a^2\psi} + \frac{b^2}{g+\beta^2\psi} + \frac{c^2}{g+\gamma^2\psi} \right) \psi$$

gesetzt ist.

Da der Exponent Sg , so wie der Ausdruck unter dem Wurzelzeichen, homogene Functionen von g und ψ sind, so sieht man sogleich, dass sich das Integral vereinfachen wird, wenn man statt einer der Variablen, etwa statt ψ , ihr Verhältniss zur anderen als neue Variable einführt. Man setze also:

$$\psi = \frac{g}{s},$$

wo s die neue Veränderliche bezeichnet, so werden die Grenzen für diese ∞ und 0, wofür man auch 0 und ∞ nehmen kann, wenn man das Vorzeichen des Integrals ändert. Man erhält so:

$$(4) \quad -\frac{i\sqrt{\pi}}{\Gamma(\frac{1}{2}(p+1))} e^{i(2-p)\pi} \int_0^\infty \int_0^\infty \frac{s^{1-\frac{1}{2}p} g^{\frac{1}{2}p-3} \sin g}{\sqrt{\left(1+\frac{s}{a^2}\right)\left(1+\frac{s}{\beta^2}\right)\left(1+\frac{s}{\gamma^2}\right)}} e^{-Sg} dg ds,$$

wo S jetzt bloss von s abhängt, und die Form hat:

$$S = \frac{a^2}{a^2+s} + \frac{b^2}{\beta^2+s} + \frac{c^2}{\gamma^2+s}.$$

Wir haben bisher, um den Fortgang der Rechnung nicht zu unterbrechen, nachzuweisen unterlassen, worauf die Befugniss beruht, in dem Integral (2), in welchem, nach den Betrachtungen, welche dasselbe herbeigeführt haben, die beiden von einander unabhängigen Integrationen nach g und ψ den auf x, y, z bezüglichen vorangehen sollten, diese Ordnung der Operationen umzukehren. Man überzeugt sich von der Berechtigung zu dieser Veränderung, wenn man im Integral (2) die Function unter dem fünffachen Zeichen mit:

$$e^{-\varepsilon\psi^2(g+\psi)}$$

multiplicirt, wo ε eine positive Constante bezeichnet, wodurch das Integral zu einem völlig bestimmten wird. Es leuchtet zunächst ein, dass das so modificirte Integral, in welchem die Integrationen nach g und ψ leicht ausgeführt werden können, für unendlich kleine Werthe von ε , das Integral (2), wie dieses eigentlich genommen werden sollte, zur Grenze hat. Beginnt man hingegen in dem modificirten Integral mit den Integrationen nach x, y, z , die sich ebenfalls

leicht bewerkstelligen lassen, so sieht man ohne Schwierigkeit, dass das daraus hervorgehende doppelte Integral den Ausdruck (3), welcher von jeder Unbestimmtheit frei ist, zur Grenze hat, womit die verlangte Nachweisung geleistet ist. Die Ausführung der eben gegebenen Andeutung ist zu leicht, als dass es nöthig sein sollte, in weiteres Detail darüber einzugehen.

Differenziren wir jetzt das Integral (4) nach a , welche Constante bloss in S vorkommt, und bringen den Factor $e^{A(2-p)\pi}$ unter das auf die Variable s sich beziehende Integrationszeichen, so erhalten wir:

$$\frac{2a}{a^2} \frac{\sqrt{\pi}}{\Gamma(\frac{1}{2}(p+1))} \int_0^\infty \frac{s^{1-p}}{\sqrt{\left(1 + \frac{s}{a^2}\right)^2 \left(1 + \frac{s}{\beta^2}\right) \left(1 + \frac{s}{\gamma^2}\right)}} R ds,$$

wobei zur Abkürzung:

$$R = e^{A(2-p)\pi} \int_0^\infty \sin q e^{Sq} q^{1-p-2} dq$$

gesetzt worden. Da der reelle Theil dieses Doppelintegrals die gesuchte Componente A darstellt, so kommt Alles darauf hinaus, den von R zu erhalten. Man findet aber diesen letzteren sogleich, wenn man $\sin q$ durch imaginäre Exponentialgrößen ausdrückt und dann die beiden Integrale, in welche R durch diese Substitution zerfällt, mit der schon häufig angeführten Gleichung des §. 3 vergleicht. Man erhält so das Resultat, dass der reelle Theil von R Null oder:

$$\frac{1}{2} \Gamma(\frac{1}{2}p-1) \sin(\frac{1}{2}p-1)\pi \cdot (1-S)^{1-\frac{1}{2}p} = \frac{\pi}{2 \Gamma(2-\frac{1}{2}p)} (1-S)^{1-\frac{1}{2}p}$$

ist, je nachdem $S > 1$ oder $S < 1$ ist.

Um nun zum Resultate in seiner definitiven Form zu gelangen, hat man zu unterscheiden, ob der angezogene Punkt im inneren oder im äusseren Raume liegt.

I. Für einen inneren Punkt hat man:

$$\frac{a^2}{\alpha^2} + \frac{b^2}{\beta^2} + \frac{c^2}{\gamma^2} < 1,$$

und folglich auch:

$$S = \frac{a^2}{a^2+s} + \frac{b^2}{\beta^2+s} + \frac{c^2}{\gamma^2+s} < 1,$$

da s nur positive Werthe erhält. Es ist mithin:

$$A = \frac{a}{a^2} \frac{\pi^{\frac{3}{2}}}{\Gamma(\frac{1}{2}(p+1))\Gamma(2-\frac{1}{2}p)} \int_0^x \frac{s^{1-\frac{1}{2}p}}{\left(1+\frac{s}{a^2}\right)^3 \left(1+\frac{s}{\beta^2}\right) \left(1+\frac{s}{\gamma^2}\right)} (1-S)^{1-\frac{1}{2}p} ds.$$

II. Ist der Punkt ein äusserer, so hat man:

$$\frac{a^2}{\alpha^2} + \frac{b^2}{\beta^2} + \frac{c^2}{\gamma^2} > 1.$$

d. h. $S > 1$, für $s = 0$. Da nun offenbar S um so kleiner ist, je grösser s ist, und für $s = \infty$ verschwindet, so giebt es einen und nur einen positiven Werth von s , für welchen $S = 1$ ist. Nennt man s_1 diesen Werth, d. h. die positive Wurzel der Gleichung:

$$\frac{a^2}{a^2+s} + \frac{b^2}{\beta^2+s} + \frac{c^2}{\gamma^2+s} = 1,$$

so hat man $S > 1$ oder < 1 , je nachdem $s < s_1$ oder $s > s_1$ ist. Das Integral erstreckt sich daher nur von $s = s_1$ bis $s = \infty$, und man erhält:

$$A = \frac{a}{a^2} \frac{\pi^{\frac{3}{2}}}{\Gamma(\frac{1}{2}(p+1))\Gamma(2-\frac{1}{2}p)} \int_{s_1}^{\infty} \frac{s^{1-\frac{1}{2}p}}{\left(1+\frac{s}{a^2}\right)^3 \left(1+\frac{s}{\beta^2}\right) \left(1+\frac{s}{\gamma^2}\right)} (1-S)^{1-\frac{1}{2}p} ds.$$

III. Wir haben, der etwas leichteren Rechnung wegen, die Differentiation an dem noch nicht auf ein einfaches Integral zurückgeführten Ausdruck (4) vollzogen. Hätte man umgekehrt die Differentiation erst nach Ausföhrung der auf g bezüglichen Integration ausgeföhrt, so würde man zu denselben Resultaten gelangt sein. Man hat auf diesem etwas längeren Wege den Vortheil, das ursprüngliche Integral (1), dessen Differentialquotienten zur Kenntniss der Attractionscomponenten allein erforderlich sind, selbst zu bestimmen. Da der Werth dieses Integrals zuweilen gebraucht werden kann, so wollen wir ihm, der Vollständigkeit wegen, so wie er aus der angedeuteten Rechnung hervorgeht, hier noch beifügen. Man findet:

$$\int \frac{dx dy dz}{q^{p-1}} = \frac{\pi^{\frac{3}{2}}}{\Gamma(\frac{1}{2}(p-1))\Gamma(3-\frac{1}{2}p)} \int_0^x \frac{s^{1-\frac{1}{2}p}}{\left(1+\frac{s}{a^2}\right) \left(1+\frac{s}{\beta^2}\right) \left(1+\frac{s}{\gamma^2}\right)} (1-S)^{2-\frac{1}{2}p} ds,$$

wo die nicht angegebene untere Grenze den Werth Null oder s_1 hat, je nachdem der angezogene Punkt ein innerer oder ein äusserer ist.

§. 6. *)

Unter den im Vorhergehenden nicht behandelten Problemen, worauf sich dieselbe Methode anwendbar erweist, verdienen diejenigen eine besondere Erwähnung, welche die Theorie der Attraction in dem Falle darbietet, wo man die auf einander wirkenden Massen beide als ausgedehnt betrachtet. Sind dv und dv' zwei beliebige Volumenelemente der beiden als homogen angenommenen Massen, bezeichnet ρ die gegenseitige Entfernung dieser Elemente, und $f(\rho)$ eine durch das Attractionsgesetz bestimmte Function, so hängt bekanntlich die vollständige Kenntniss der Wirkung, welche die Massen auf einander ausüben, von dem sechsfachen Integrale ab:

$$\int \int f(\rho) dv dv'.$$

welches über beide Massen auszudehnen ist, indem die sechs zu jener Kenntniss erforderlichen Grössen leicht durch die Differentialquotienten nach den sechs in den Grenzen des Integrals enthaltenen Constanten ausgedrückt werden, welche sich auf die relative Lage der beiden Massen beziehen. Das sechsfache Integral lässt sich allgemein auf ein vierfaches zurückführen**), welches sich über die Oberflächen beider Körper erstreckt, wenn man gewisse einfache von der Function $f(\rho)$ abhängige Integrale als bekannt voraussetzt. Eine weitere Reduction des vierfachen Integrals wird nur für Körper von besonderer Gestalt und für ein bestimmtes Gesetz der Elementarwirkung stattfinden können; aber selbst auf solche specielle Fälle, wenn sie nicht zu den allereinfachsten gehören, wie dies z. B. von der Annahme gilt, wo eine der Massen als kugelförmig betrachtet wird, werden die bekannten Integrationsmethoden sehr schwer anwendbar sein. Ein Fall, für den die gewöhnlichen Mittel wenig Erfolg zu versprechen scheinen, ist der zweier Ellipsoide in ganz beliebiger Lage, deren Elemente sich nach dem im vorigen Paragraphen zu Grunde gelegten Gesetze anziehen. Wendet man hingegen auf dieses Problem unsere Methode an, so findet man ohne Schwierigkeit, dass das sechsfache Integral auf ein doppeltes zurückgeführt werden kann, welches sehr verschiedenartiger Formen fähig ist, welche theils von den in den ursprünglichen Ausdruck eingeführten Hilfsintegralen, theils

*) Dieser letzte Paragraph befand sich nicht in der ursprünglichen Abhandlung und ist erst während des Druckes hinzugefügt worden.

**) Principia generalia theoriae figurae fluidorum in statu aequilibrii. auct. C. F. GAUSS, art. 6 et seq.

auch von der Wahl der Coordinaten abhängen, durch welche man sich die Elemente dv und dv' ausgedrückt denkt. Die einfachste und am meisten symmetrische Form des Endresultats scheint die zu sein, welche aus der Annahme eines geeigneten Systems schiefwinkliger Coordinaten hervorgeht. Nach einem bekannten Satze, welcher von MONGE herrührt und zuerst von CHASLES bewiesen worden ist*), haben zwei Flächen zweiten Grades mit Mittelpunkten immer ein der Richtung nach gemeinsames System von conjugirten Durchmessern. Nimmt man die Axen diesen Durchmessern parallel und legt zugleich den Anfangspunkt in die Mitte der Geraden, welche beide Mittelpunkte verbindet, so sind die Gleichungen für die Ellipsoide:

$$\left(\frac{x+a}{a}\right)^2 + \left(\frac{y+b}{\beta}\right)^2 + \left(\frac{z+c}{\gamma}\right)^2 = 1, \quad \left(\frac{x'-a}{a'}\right)^2 + \left(\frac{y'-b}{\beta'}\right)^2 + \left(\frac{z'-c}{\gamma'}\right)^2 = 1,$$

und die Rechnung gestaltet sich für beide ganz symmetrisch. Da das Resultat, welches diesem Ausgangspunkt entspricht, durch seine Form einiges Interesse darzubieten scheint, so wird es vielleicht nicht unpassend sein, wenn wir die Rechnungen, welche zu demselben führen, bei einer anderen Gelegenheit ausführlich entwickeln.

*) Correspondance sur l'École Polytechnique, Vol. III p. 328.

RECHERCHES SUR DIVERSES APPLICATIONS
DE L'ANALYSE INFINITÉSIMALE
A LA THÉORIE DES NOMBRES.

PAR

M. G. LEJEUNE DIRICHLET.

Crelle, Journal für die reine und angewandte Mathematik. Bd. 19 S. 324—369,
Bd. 21 S. 1—12 und S. 134—155.

RECHERCHES SUR DIVERSES APPLICATIONS DE L'ANALYSE INFINITÉSIMALE A LA THÉORIE DES NOMBRES.

En m'occupant, il y a deux ans^{*)}, à prouver que toute progression arithmétique indéfinie dont les termes n'ont pas tous un même diviseur commun, renferme une infinité de nombres premiers, ce qui n'avait pas encore été fait d'une manière rigoureuse, j'ai été conduit à envisager un grand nombre de questions relatives aux nombres, sous un point de vue entièrement nouveau, et qui les rattache aux principes de l'analyse infinitésimale et aux propriétés remarquables d'une classe de séries et de produits infinis qui ont beaucoup d'analogie avec les expressions que l'illustre EULER a considérées dans le chapitre de son Introduction à l'analyse de l'infini, ayant pour titre „De seriebus ex evolutione factorum ortis.“ Dans une note insérée dans le Journal de CRELLE**), j'ai déjà indiqué plusieurs des questions auxquelles ce genre d'analyse peut être appliqué. Je me propose maintenant d'exposer mes recherches sur cette matière avec tous les développements nécessaires, dans une suite de mémoires dont celui que je soumetts aujourd'hui au jugement des géomètres, sera particulièrement destiné à l'examen d'une question dont la solution n'avait pas encore été donnée, et qui a pour objet de déterminer le nombre des formes quadratiques différentes dont le déterminant D est un entier quelconque positif ou négatif, ou ce qui est la même chose, le nombre des diviseurs quadratiques qui appartiennent à l'expression $x^2 - Dy^2$. L'analyse qui nous conduira à la solution complète de cette question intéressante, nous fournira en même temps et pour ainsi dire, chemin faisant, des démonstrations nouvelles et très simples de plusieurs beaux théorèmes dus à M. GAUSS, mais que cet illustre géomètre

^{*)} Le mémoire que j'ai lu sur cette question à l'Académie de Berlin, vient d'être imprimé dans la collection de l'Académie, année 1837.)

^{**)} Tome XVIII, p. 259.)

¹⁾ S. 313 dieser Ausgabe von G. Lejeune Dirichlet's Werken. ²⁾ S. 357 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

n'avait établis qu'au moyen de considérations très compliquées dans la seconde partie de la 5^{me} section de ses *Disquisitiones arithmeticae*.

Cette section de l'ouvrage de M. GAUSS, qui est consacrée à la théorie des formes du second degré, se compose de deux parties très distinctes, dont la première, qui se termine à l'art. 223, peut être considérée comme l'exposition de la partie élémentaire de cette théorie, et renferme tous les résultats antérieurement donnés par EULER, LAGRANGE et LEGENDRE, complétés et étendus à beaucoup d'égards et déduits d'ailleurs de principes nouveaux. La seconde partie qui commence, à proprement parler, à l'art. 234, (les art. 223—233 contenant des définitions et des lemmes qui servent d'introduction à la seconde partie) se compose presque exclusivement de recherches propres à l'illustre auteur. Ces recherches, aussi remarquables par la profondeur des méthodes que par le nombre et la variété des résultats, forment sans contredit la partie de tout l'ouvrage dont l'étude présente le plus de difficultés. Aussi sont-elles très peu connues des géomètres, et l'on doit y rapporter particulièrement ce que LEGENDRE dit dans la préface de la seconde édition de sa *Théorie des Nombres*, lorsqu'après avoir indiqué les découvertes de M. GAUSS qu'il avait fait entrer dans son ouvrage, il ajoute :

„On aurait désiré enrichir cet Essai d'un plus grand nombre des excellents matériaux qui composent l'ouvrage de M. GAUSS: mais les méthodes de cet auteur lui sont tellement particulières qu'on n'aurait pu, sans des circuits très étendus, et sans s'assujettir au simple rôle de traducteur, profiter de ses autres découvertes.“

J'ose donc espérer qu'indépendamment des résultats nouveaux qu'il fait connaître, mon travail pourra encore contribuer à l'avancement de la science, en établissant sur de nouvelles bases et en rapprochant des éléments, de belles et importantes théories qui n'ont été jusqu'à présent à la portée que du petit nombre de géomètres capables de la contention d'esprit nécessaire pour ne pas perdre le fil des idées dans une longue suite de calculs et de raisonnements très composés.

§. 1.

Les lettres k et ρ désignant deux quantités positives, la première constante, la seconde variable, considérons la somme de la série infinie :

$$(1) \quad \frac{1}{k+\rho} + \frac{1}{(k+1)^{\rho+\rho}} + \frac{1}{(k+2)^{\rho+\rho}} + \dots$$

Cette somme croissant au delà de toute limite finie, lorsque la variable ϱ devient infiniment petite, voyons quelle est la fonction de ϱ la plus simple qui puisse servir de mesure à cette augmentation, ou en d'autres termes, dont le rapport à l'expression précédente converge vers l'unité, lorsque ϱ convergera vers zéro. Pour cela, nous aurons recours à la formule connue:

$$\int_0^1 x^{k-1} \log^{\varrho} \left(\frac{1}{x} \right) dx = \frac{\Gamma(1+\varrho)}{k^{1+\varrho}}.$$

En mettant successivement $k, k+1, k+2, \dots$ à la place de k et faisant la somme de toutes ces équations, la série (1) se trouvera exprimée comme il suit:

$$\frac{1}{\Gamma(1+\varrho)} \int_0^1 \frac{x^{k-1}}{1-x} \log^{\varrho} \left(\frac{1}{x} \right) dx.$$

Si l'on ajoute $\frac{1}{\varrho}$ à cette expression et que l'on en retranche la quantité égale:

$$\frac{\Gamma(\varrho)}{\Gamma(1+\varrho)} = \frac{1}{\Gamma(1+\varrho)} \int_0^1 \log^{\varrho-1} \left(\frac{1}{x} \right) dx,$$

elle deviendra:

$$\frac{1}{\varrho} + \frac{1}{\Gamma(1+\varrho)} \int_0^1 \left[\frac{x^{k-1}}{1-x} - \frac{1}{\log \left(\frac{1}{x} \right)} \right] \log^{\varrho} \left(\frac{1}{x} \right) dx.$$

Comme le second terme converge vers la limite finie:

$$\int_0^1 \left[\frac{x^{k-1}}{1-x} - \frac{1}{\log \left(\frac{1}{x} \right)} \right] dx,$$

k étant > 0 , on conclut que le rapport de la somme (1) à la fraction $\frac{1}{\varrho}$ a l'unité pour limite, lorsque la variable positive ϱ devient moindre que toute grandeur donnée.

Au moyen du résultat précédent, il nous sera facile de démontrer le théorème suivant, dont nous ferons un usage très fréquent dans nos recherches.

Soient:

$$(2) \quad l_1, l_2, l_3, \dots, l_n, \dots$$

des constantes en nombre infini, positives, différentes de zéro, inégales ou en partie égales; soit encore $f(t)$ une fonction discontinue de la variable positive t , qui exprime combien il y a dans la suite (2) de termes dont la valeur ne surpasse pas celle de t . Cela posé, si la fonction $f(t)$ peut être mise sous

la forme:

$$(3) \quad f(t) = ct + t^\gamma \psi(t),$$

c et γ désignant des constantes positives dont la seconde est inférieure à l'unité, et la nouvelle fonction $\psi(t)$, abstraction faite de son signe et quelque grande qu'on y suppose la variable t , restant toujours moindre que la constante positive C , je dis que la somme:

$$(4) \quad g(\varrho) = \frac{1}{l_1^{1+\varrho}} + \frac{1}{l_2^{1+\varrho}} + \frac{1}{l_3^{1+\varrho}} + \dots,$$

dans laquelle ϱ désigne une variable positive, sera telle qu'on aura pour une valeur infiniment petite de ϱ :

$$(5) \quad g(\varrho) = \frac{c}{\varrho}.$$

c'est-à-dire que le rapport de la somme $g(\varrho)$ à la fraction $\frac{c}{\varrho}$ convergera vers l'unité, lorsque ϱ devient moindre que toute grandeur donnée.

Le nombre des termes de la suite (2) qui ne surpassent pas l'unité, est limité (ce nombre étant égal à $c + \psi(1)$), et comme parmi ces termes il n'y en a aucun dont la valeur soit zéro, il est évident par la nature de la proposition qu'il s'agit d'établir, que nous pouvons omettre la partie de l'expression $g(\varrho)$, qui correspond à ces termes. Ce qui reste après ce retranchement, étant toujours désigné par $g(\varrho)$, choisissons une constante δ supérieure à $\frac{1}{1-\gamma}$, et partageons la somme $g(\varrho)$ en une infinité de sommes partielles, en comprenant dans la $m^{\text{ième}}$ de ces sommes partielles tous les termes qui satisfont à la double condition:

$$m^\delta < l_n \leq (m+1)^\delta,$$

et par suite à celle-ci:

$$\frac{1}{m^{\delta(1+\varrho)}} > \frac{1}{l_n^{1+\varrho}} \geq \frac{1}{(m+1)^{\delta(1+\varrho)}}.$$

Le nombre de ces termes sera évidemment:

$$f((m+1)^\delta) - f(m^\delta).$$

La valeur numérique de $t^\gamma \psi(t)$, lorsqu'on suppose successivement $t = m^\delta$ et $t = (m+1)^\delta$, étant inférieure à $C(m+1)^{\gamma\delta}$, on aura ces deux inégalités:

$$\begin{aligned} f((m+1)^\delta) - f(m^\delta) &< c((m+1)^\delta - m^\delta) + 2C(m+1)^{\gamma\delta} \\ f((m+1)^\delta) - f(m^\delta) &> c((m+1)^\delta - m^\delta) - 2C(m+1)^{\gamma\delta}. \end{aligned}$$

En combinant ces inégalités avec celles que nous venons d'écrire, on conclura que la somme partielle dont il s'agit, est respectivement inférieure et supérieure aux quantités :

$$c \frac{(m+1)^\delta - m^\delta}{m^{\delta(1+\varrho)}} + 2c \frac{(m+1)^{\gamma\delta}}{m^{\delta(1+\varrho)}} \cdot c \frac{(m+1)^\delta - m^\delta}{(m+1)^{\delta(1+\varrho)}} - 2c \frac{(m+1)^{\gamma\delta}}{(m+1)^{\delta(1+\varrho)}}.$$

Il suit de là qu'on a :

$$g(\varrho) < c \Sigma \frac{(m+1)^\delta - m^\delta}{m^{\delta(1+\varrho)}} + 2c \Sigma \frac{(m+1)^{\gamma\delta}}{m^{\delta(1+\varrho)}},$$

le signe Σ s'étendant depuis $m = 1$ jusqu'à $m = \infty$.

Puisqu'on a en vertu d'un théorème connu :

$$(m+1)^\delta - m^\delta = \delta m^{\delta-1} + \frac{\delta(\delta-1)}{2} (m+\varepsilon_m)^{\delta-2}.$$

ε_m désignant une fraction positive, l'inégalité précédente pourra se mettre sous la forme :

$$g(\varrho) < c\delta \Sigma \frac{1}{m^{1+\delta\varrho}} + \frac{1}{2} c\delta(\delta-1) \Sigma \left(1 + \frac{\varepsilon_m}{m}\right)^\delta \frac{1}{m^{\delta\varrho}(m+\varepsilon_m)^2} + 2c \Sigma \left(1 + \frac{1}{m}\right)^{\gamma\delta} \frac{1}{m^{\delta(1-\gamma)+\delta\varrho}}.$$

Or, ϱ devenant infiniment petit, les deux dernières sommes resteront finies, car elles seront constamment inférieures à celles-ci :

$$\Sigma \left(1 + \frac{1}{m}\right)^\delta \frac{1}{m^2}, \quad \Sigma \left(1 + \frac{1}{m}\right)^{\gamma\delta} \frac{1}{m^{\delta(1-\gamma)}}.$$

qui le sont elles-mêmes, comme il est facile de le voir au moyen des principes connus, si l'on se rappelle que, d'après la supposition faite sur la constante δ , on a $\delta(1-\gamma) > 1$. Quant à la première somme, comme elle a une forme analogue à l'expression (1) considérée plus haut, elle sera évidemment $\frac{1}{\delta\varrho}$. ϱ étant supposé infiniment petit. On voit donc que la limite supérieure de $g(\varrho)$ prend la forme $\frac{c}{\varrho}$, lorsque ϱ devient moindre que toute grandeur donnée, et comme le même raisonnement peut s'appliquer à la limite inférieure et conduit au même résultat, la proposition énoncée se trouve établie.

On pourrait donner au théorème que nous venons de démontrer, beaucoup plus d'étendue, mais comme ce théorème tel que nous l'avons énoncé, suffit aux applications que nous avons en vue, quant à présent, nous ne nous arrêterons pas à cette généralisation qui ne présente d'ailleurs aucune difficulté.

Nous aurons encore besoin de deux autres lemmes qui appartiennent, comme le précédent, à l'analyse infinitésimale. Le premier de ces nouveaux lemmes est tellement simple que nous nous contenterons de l'énoncer, sans en donner la démonstration qui est très facile à suppléer.

Tous les points d'un plan infini étant rapportés à deux axes rectangulaires des x et des y , concevons dans ce plan une courbe fermée assujettie ou non à une même loi analytique dans toutes ses parties, supposons que les dimensions de cette courbe augmentent de plus en plus et au-delà de toute limite, de manière cependant que la courbe variable reste toujours semblable à elle-même, et désignons par σ l'aire également variable à laquelle la courbe sert de contour.

Soient maintenant a, b, α, β quatre constantes dont les deux premières ont des valeurs positives, et supposons que l'on construise tous les points dont les coordonnées x et y ont la forme :

$$(6) \quad x = av + \alpha, \quad y = bw + \beta,$$

où v et w désignent tous les entiers depuis $-\infty$ jusqu'à ∞ . Cela posé, si l'on désigne par $F(\sigma)$ le nombre de ces points situés dans l'intérieur de la courbe, on aura évidemment pour des valeurs infinies de σ :

$$F(\sigma) = \frac{1}{ab} \sigma,$$

c'est-à-dire que le rapport des deux membres de cette équation convergera vers l'unité lorsque σ croît au-delà de toute limite positive. Il est également facile de voir que la différence $F(\sigma) - \frac{\sigma}{ab}$ croîtra moins rapidement que la puissance σ^γ , l'exposant γ étant supposé $> \frac{1}{2}$. Nous pouvons donc poser :

$$(7) \quad F(\sigma) = \frac{1}{ab} \sigma + \sigma^\gamma \psi(\sigma),$$

où l'on a $\frac{1}{2} < \gamma < 1$, et l'on sera assuré que la fonction $\psi(\sigma)$, abstraction faite de son signe, restera toujours moindre qu'une certaine constante finie C .

Le dernier des lemmes que nous emprunterons à l'analyse infinitésimale, se rapporte à la théorie des séries. On sait que les séries infinies convergentes sont de deux espèces très différentes, les séries de la première espèce étant convergentes indépendamment des signes dont leurs termes sont affectés, tandis que celles de la seconde ne jouissent de cette propriété que parce que les termes se détruisent en partie par l'opposition de leurs signes.

La convergence d'une série de la première espèce subsiste et sa somme conserve toujours la même valeur, quel que soit l'ordre que l'on établit entre ses termes. Les séries de la seconde espèce se comportent d'une manière entièrement différente. Une série de cette espèce, convergente pour un certain arrangement de ses termes, peut perdre cette propriété lorsque cet ordre vient à être changé. Il peut arriver aussi que la série soit encore convergente après ce changement, mais que sa somme ait varié en même temps que l'ordre de ses termes. Ces remarques intimement liées à notre sujet, comme on le verra plus loin, ne sont pas sans importance pour d'autres recherches. Il en résulte par exemple et pour le dire en passant, que si l'on parvient à sommer une série qui appartient à la seconde espèce, et que l'on trouve pour la somme de la série une valeur entièrement déterminée, sans que l'ordre dans lequel les termes sont supposés se suivre, entre comme un élément essentiel dans l'analyse dont on fait usage, la méthode de sommation doit renfermer quelque vice caché, ou du moins a besoin d'être complétée par quelque considération qui indique clairement quel est l'arrangement des termes auquel la somme obtenue correspond.

Pour revenir à notre objet, soit s une variable positive et considérons la série dont le terme général est:

$$c_n \frac{1}{n^s},$$

l'entier n étant susceptible de toutes les valeurs depuis $n = 1$ jusqu'à $n = \infty$. Si nous supposons que c_n , abstraction faite de son signe, et quel que soit l'indice n , soit toujours moindre que la constante C , notre série appartiendra à la première espèce tant que l'on aura $s > 1$. En posant donc $s = 1 + \varrho$, ϱ étant une variable positive aussi petite que l'on voudra, la somme:

$$\psi(1 + \varrho) = \sum c_n \frac{1}{n^{1+\varrho}}$$

aura une valeur unique et entièrement indépendante de l'arrangement de ses termes. Concevons maintenant qu'il s'agisse d'obtenir la limite vers laquelle la fonction $\psi(1 + \varrho)$, évidemment continue tant que la variable ϱ reste positive, converge lorsque ϱ devient moindre que toute grandeur donnée, en supposant toutefois qu'une pareille limite existe, ce qui peut n'avoir pas lieu. D'après les remarques faites plus haut, on ne serait pas fondé à dire que cette limite

soit exprimée par :

$$\sum c_n \frac{1}{n}.$$

l'ordre des termes étant arbitraire, car il est évident que cette dernière série appartient à la seconde espèce, et n'a par conséquent pas de somme déterminée.

Les suppositions énoncées plus haut étant conservées, soit k un entier positif, et concevons que c_n satisfasse à l'équation :

$$(8) \quad c_{n+k} = c_n.$$

ou en d'autres termes, que la suite :

$$c_1, c_2, \dots, c_k; c_{k+1}, c_{k+2}, \dots, c_{2k}; c_{2k+1}, \dots$$

soit périodique, le nombre des termes qui composent une période étant égal à k . Supposons encore que la somme de ces termes soit zéro, c'est-à-dire que l'on ait :

$$(9) \quad c_1 + c_2 + \dots + c_k = 0.$$

Cela étant, je dis que la somme :

$$\sum c_n \frac{1}{n^{1+p}}$$

qui ne dépend pas de l'ordre des termes, converge vers une limite finie, donnée par l'expression :

$$\sum c_n \frac{1}{n},$$

où les termes sont supposés se suivre dans l'ordre naturel, c'est-à-dire de manière à ce que les valeurs de n croissent constamment depuis $n = 1$ jusqu'à $n = \infty$. Pour démontrer cette assertion, il suffira évidemment de faire voir que la série :

$$\sum c_n \frac{1}{n^s},$$

les termes étant rangés dans l'ordre indiqué, reste convergente et exprime une fonction continue de s , depuis $s = \infty$ jusqu'à $s = 1$ inclusivement. Or il est facile de prouver que cette double propriété subsiste non seulement entre les limites précédentes, mais plus généralement tant que s reste supérieur à zéro. En effet, h étant un entier positif quelconque, exprimons par une intégrale définie la somme des hk premiers termes de la série précédente. Au moyen de

la formule:

$$\int_0^1 x^{n-1} \log^{s-1} \left(\frac{1}{x} \right) dx = \frac{\Gamma(s)}{n^s},$$

et en ayant égard à l'équation (8), on trouvera pour cette somme:

$$\frac{1}{\Gamma(s)} \int_0^1 \frac{\sum c_n x^{n-1}}{1-x^k} \log^{s-1} \left(\frac{1}{x} \right) dx = \frac{1}{\Gamma(s)} \int_0^1 \frac{\sum c_n x^{n-1}}{1-x^k} x^{hk} \log^{s-1} \left(\frac{1}{x} \right) dx,$$

le signe sommatoire s'étendant depuis $n = 1$ jusqu'à $n = k$. Le polynôme $\sum c_n x^{n-1}$ étant divisible par $1-x$, comme on le voit par l'équation (9), la fraction algébrique sous le signe d'intégration reste finie. Soit K la plus grande valeur numérique de cette fraction depuis $x = 0$ jusqu'à $x = 1$: la seconde intégrale sera donc moindre que:

$$\frac{K}{\Gamma(s)} \int_0^1 x^{hk} \log^{s-1} \left(\frac{1}{x} \right) dx = \frac{K}{(hk+1)^s},$$

et s'évanouira pour $h = \infty$. Il résulte de là que la série prolongée à l'infini est convergente, et l'on voit avec la même facilité que sa somme exprimée par la première intégrale, est une fonction de s , qui varie d'une manière continue avec cette variable tant que l'on a $s > 0$.

§. 2.

p étant un nombre premier impair, positif ou négatif, et k un entier non-divisible par p , qui peut être aussi positif ou négatif, nous désignons avec LEGENDRE par $\left(\frac{k}{p}\right)$ l'unité prise avec le signe plus ou avec le signe moins, suivant que k sera ou ne sera pas résidu quadratique relativement à p . L'illustre auteur définit le symbole $\left(\frac{k}{p}\right)$ comme le reste que donne la puissance $k^{k(p-1)}$, lorsqu'on la divise par p ; la définition précédente, quoique la même au fond, est préférable pour notre objet en ce qu'elle ne suppose pas que p soit un nombre positif. Si nous désignons par l un second entier non-divisible par p et par q un nombre premier impair dont la valeur numérique diffère de celle de p , on aura suivant la notation précédente:

$$(1) \quad \begin{cases} \left(\frac{k}{p}\right)\left(\frac{l}{p}\right) = \left(\frac{kl}{p}\right), & \left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}, & \left(\frac{2}{p}\right) = (-1)^{\frac{1}{2}p'-1}, \\ \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)}. \end{cases}$$

Ces équations qui renferment toute la théorie des résidus quadratiques, supposent de plus, la seconde que p est positif, la quatrième que p et q n'ont pas simultanément le signe négatif.

Les entiers k et P , positifs ou négatifs, n'ayant pas de diviseur commun, et le second P , que nous supposons impair, étant décomposé en ses facteurs simples p, p', p'', \dots égaux ou inégaux, de sorte que $P = pp'p'' \dots$, nous aurons souvent à distinguer si ceux des nombres premiers p, p', p'', \dots à l'égard desquels k est non-résidu quadratique, sont en nombre pair ou impair, ou ce qui est la même chose, si le produit :

$$\left(\frac{k}{p}\right)\left(\frac{k}{p'}\right)\left(\frac{k}{p''}\right)\dots$$

a la valeur $+1$ ou -1 . M. JACOBI a proposé d'étendre la notation de LEGENDRE à de semblables produits et d'écrire :

$$\left(\frac{k}{P}\right) = \left(\frac{k}{p}\right)\left(\frac{k}{p'}\right)\left(\frac{k}{p''}\right)\dots$$

Comme cette généralisation de la notation de LEGENDRE, dont l'illustre géomètre que je viens de citer, a fait des applications ingénieuses*), est très propre à simplifier les formules et à abrégé les démonstrations, nous l'adopterons dans ce qui suivra. On aura suivant cette notation :

$$(2) \quad \left\{ \begin{array}{l} \left(\frac{k}{P}\right)\left(\frac{l}{P}\right) = \left(\frac{kl}{P}\right), \quad \left(\frac{k}{P}\right)\left(\frac{k}{Q}\right) = \left(\frac{k}{PQ}\right), \quad \left(\frac{-1}{P}\right) = (-1)^{\frac{1}{2}(P-1)}, \\ \left(\frac{2}{P}\right) = (-1)^{\frac{1}{2}(P^2-1)}, \quad \left(\frac{Q}{P}\right) = \left(\frac{P}{Q}\right)(-1)^{\frac{1}{2}(P-1)\cdot\frac{1}{2}(Q-1)}, \end{array} \right.$$

en supposant que les entiers k et l n'ont pas de diviseur commun avec les nombres impairs P et Q , que P est positif dans la troisième, et enfin que P et Q sont premiers entre eux et n'ont pas simultanément le signe négatif dans la dernière de ces équations. Toutes ces équations sont ou évidentes ou se déduisent facilement des relations (1), et il serait d'autant plus inutile de nous arrêter à les démontrer que les théorèmes qu'elles expriment se trouvent déjà, à la notation près, dans l'ouvrage de M. GAUSS art. 133. Pour éviter des distinctions inutiles il conviendra de ne pas exclure le cas où P dans le symbole $\left(\frac{k}{P}\right)$ a la valeur ± 1 , en supposant $\left(\frac{k}{\pm 1}\right) = 1$. Il est évident que cette

* Compte rendu des séances de l'Académie de Berlin, Oct. 1837.

nouvelle convention est compatible avec les équations précédentes, et qu'en l'adoptant, la troisième de ces équations se trouvera comprise dans la cinquième et répondra à $Q = -1$.

Nous terminerons ce paragraphe, en posant les équations évidentes qui suivent, et dans lesquelles k et l désignent des nombres impairs et δ la valeur ± 1 :

$$(3) \quad \delta^{\frac{1}{2}(k-1)} \delta^{\frac{1}{2}(l-1)} = \delta^{\frac{1}{2}(k+l-1)}, \quad \delta^{\frac{1}{2}(k^2-1)} \delta^{\frac{1}{2}(l^2-1)} = \delta^{\frac{1}{2}(kl^2-1)}.$$

§. 3.

Nous avons maintenant à rappeler quelques résultats connus qui se rapportent à la théorie des formes quadratiques. En désignant par D un entier positif ou négatif (le cas de $D = 0$ sera excepté), nous appellerons avec M. GAUSS forme du déterminant D , toute expression comme:

$$ax^2 + 2bxy + cy^2,$$

a, b, c étant des entiers donnés, liés entre eux par la condition $b^2 - ac = D$, et x et y désignant des entiers indéterminés. Lorsque le déterminant D est un nombre négatif, les coefficients extrêmes seront toujours de même signe. Nous ne considérons, dans ce cas, que les formes pour lesquelles ce signe est $+$, c'est-à-dire les formes qui n'expriment que des nombres positifs. M. GAUSS range les formes qui appartiennent à un même déterminant en différents ordres, en comprenant dans un même ordre toutes celles pour lesquelles le plus grand diviseur commun de a, b, c a la même valeur. Nous supposons toujours qu'un pareil diviseur n'existe pas ou plutôt qu'il est égal à l'unité, les autres cas pouvant être immédiatement ramenés à celui-ci. Les formes dont il s'agit et dont l'ensemble forme l'ordre appelé primitif, peuvent elles-mêmes présenter deux cas. Il peut arriver que a et c soient simultanément pairs ou que cette condition n'ait pas lieu. Dans le second de ces cas, les formes constituent ce que M. GAUSS appelle l'ordre proprement primitif, l'autre cas étant celui de l'ordre improprement primitif. Quand nous parlerons de formes quadratiques sans autre désignation, nous sous-entendrons toujours que ces formes appartiennent à l'ordre proprement primitif. On sait d'ailleurs que l'ordre improprement primitif n'existe que lorsqu'on a $D \equiv 1 \pmod{4}$.

Deux formes:

$$ax^2 + 2bxy + cy^2, \quad a'x'^2 + 2b'x'y' + c'y'^2$$

étant telles que la première se change dans la seconde, au moyen de la sub-

stitution:

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y',$$

où l'on a :

$$\alpha\delta - \beta\gamma = \pm 1,$$

sont dites équivalentes et cette équivalence est appelée propre ou impropre, suivant que le signe supérieur ou le signe inférieur a lieu. Cette distinction que M. GAUSS a introduite dans la théorie des formes quadratiques, et qui est analogue à celle que l'on fait en géométrie entre l'égalité par superposition et l'égalité par symétrie^{*)}, a beaucoup d'importance en ce qu'elle conserve à la théorie des formes du second degré une simplicité que cette théorie n'aurait pas, à beaucoup près, si l'on n'y avait pas égard. Nous n'aurons pas à considérer l'équivalence impropre; en disant donc simplement que deux formes sont équivalentes, nous sous-entendons toujours qu'il s'agit de l'équivalence propre.

Les formes (positives et proprement primitives) dont le déterminant est un nombre donné D , et qui sont toujours en nombre infini, peuvent se distribuer en un nombre limité de classes, en plaçant deux formes dans la même classe ou dans des classes différentes suivant que ces formes sont ou ne sont pas équivalentes. Si l'on prend dans chaque classe l'une quelconque des formes qui la composent, on aura ce que nous appellerons le système complet des formes différentes, ou plus simplement, les formes différentes du déterminant D . Ce système étant construit, il est évident que toute forme dont le déterminant est D , aura toujours son équivalente et n'en aura qu'une dans ce système. Il est également facile de voir que si l'on construit un système semblable pour l'ordre des formes improprement primitives, ce nouveau système jouira de la même propriété relativement à toute forme qui appartient au même ordre.

Les formes différentes qui correspondent au déterminant quelconque D , sont divisées par M. GAUSS en genres, qui sont analogues à ce que LEGENDRE appelle groupes de diviseurs quadratiques. La différence qui existe à cet égard entre les illustres géomètres que je viens de citer, tient uniquement à ce que LEGENDRE exclut les déterminants qui ont des diviseurs carrés, ce que M. GAUSS

^{*)} On peut consulter sur cette analogie remarquable un article que M. GAUSS a inséré dans les annonces littéraires de Gottingue et dans lequel l'illustre auteur, après avoir rendu compte d'un ouvrage de M. SEEBER sur les formes quadratiques à trois indéterminées, entre dans des détails très intéressants, sur la manière dont on peut représenter géométriquement les propriétés des formes du second degré qui renferment deux ou trois entiers indéterminés.¹⁾

¹⁾ Gauss' Werke, Band II, S. 188—196. K.

ne fait pas et ce que nous ne ferons pas non plus, la considération des déterminants de cette espèce étant indispensable dans différentes recherches. Voici maintenant les principes très faciles à établir, sur lesquels repose la division en genres. (Disq. arithm. art. 229 et suivants.)

I. Si l est un nombre premier impair qui divise D , les entiers m , non-divisibles par l , qui peuvent être représentés par une même forme ayant D pour déterminant, sont ou tous tels que $\left(\frac{m}{l}\right) = 1$, ou tous tels que $\left(\frac{m}{l}\right) = -1$.

II. Lorsqu'on a $D \equiv 3 \pmod{4}$, les nombres impairs m susceptibles d'être représentés par la même forme, sont ou tous tels que $(-1)^{\frac{1}{2}(m-1)} = 1$, ou tous tels que $(-1)^{\frac{1}{2}(m-1)} = -1$.

III. Lorsqu'on a $D \equiv 2 \pmod{8}$, les nombres impairs m susceptibles d'être représentés par la même forme, sont ou tous tels que $(-1)^{\frac{1}{2}(m^2-1)} = 1$, ou tous tels que $(-1)^{\frac{1}{2}(m^2-1)} = -1$.

IV. Lorsqu'on a $D \equiv 6 \pmod{8}$, les nombres impairs m susceptibles d'être représentés par la même forme, sont ou tous tels que $(-1)^{\frac{1}{2}(m-1) + \frac{1}{2}(m^2-1)} = 1$, ou tous tels que $(-1)^{\frac{1}{2}(m-1) + \frac{1}{2}(m^2-1)} = -1$.

V. Lorsqu'on a $D \equiv 4 \pmod{8}$, les nombres impairs m susceptibles d'être représentés par la même forme, sont ou tous tels que $(-1)^{\frac{1}{2}(m-1)} = 1$, ou tous tels que $(-1)^{\frac{1}{2}(m-1)} = -1$.

VI. Lorsqu'on a $D \equiv 0 \pmod{8}$, les nombres impairs m susceptibles d'être représentés par la même forme, sont tous exclusivement contenus dans l'une de ces quatre formes $8\mu + 1, 3, 5, 7$, ou ce qui revient au même, on a à la fois $(-1)^{\frac{1}{2}(m-1)} = \pm 1$, $(-1)^{\frac{1}{2}(m^2-1)} = \pm 1$, chacun des deux signes ambigus restant invariable pour la même forme.

Toute propriété de la nature de celles exprimées dans les énoncés précédents, est ce que M. GAUSS appelle un caractère particulier de la forme à laquelle cette propriété appartient. C'est ainsi que les caractères particuliers de la forme $5x^2 + 4xy + 14y^2$, dont le déterminant est $-66 = -2.3.11$, sont contenus dans les équations:

$$\left(\frac{m}{3}\right) = -1, \quad \left(\frac{m}{11}\right) = 1, \quad (-1)^{\frac{1}{2}(m-1) + \frac{1}{2}(m^2-1)} = -1.$$

L'ensemble des caractères particuliers d'une forme constitue son caractère complet, et la distribution des formes en genres consiste à rapporter au

même genre les formes qui ont le même caractère complet, et à des genres différents celles dont les caractères complets sont différents. Quant au nombre des genres différents, ou ce qui est la même chose, des caractères complets différents, il est, généralement parlant, moindre que celui des combinaisons que l'on peut former avec les caractères particuliers différents, puisqu'il existe toujours, à l'exception d'un cas singulier, une relation entre les caractères particuliers qui conviennent à la même forme quadratique, relation qui dérive des théorèmes (2) du paragraphe précédent. Pour voir en quoi consiste cette relation, soit S^2 le plus grand carré qui divise D , et désignons par P ou par $2P$ le quotient $\frac{D}{S^2}$, suivant qu'il est impair ou pair. Nous aurons donc selon ces deux cas :

$$D = PS^2, \quad \text{ou} \quad D = 2PS^2,$$

et le nombre impair P étant décomposé en ses facteurs simples p, p', p'', \dots :

$$P = pp'p'' \dots$$

ces facteurs seront tous inégaux. Si nous considérons maintenant une forme quelconque, appartenant à l'ordre proprement primitif et ayant D pour déterminant, on pourra toujours attribuer aux indéterminées x et y des valeurs premières entre elles et telles que la valeur correspondante m de la forme soit positive, impaire et première à D . Cela étant, D sera résidu quadratique relativement à m et par suite aussi à l'égard de tous les facteurs simples de m . (Disq. arithm. art. 154.) On aura donc $\left(\frac{D}{m}\right) = 1$, et par conséquent suivant les deux cas que nous venons de distinguer :

$$\left(\frac{P}{m}\right) = 1, \quad \text{ou} \quad \left(\frac{2P}{m}\right) = \left(\frac{2}{m}\right)\left(\frac{P}{m}\right) = 1.$$

D'un autre côté, m étant positif, il résulte des équations (2) §. 2 :

$$\left(\frac{P}{m}\right) = \left(\frac{m}{P}\right)(-1)^{\frac{1}{2}(P-1)\frac{1}{2}(m-1)}.$$

Si l'on remarque maintenant que la puissance $(-1)^{\frac{1}{2}(P-1)\frac{1}{2}(m-1)}$ est équivalente à 1, ou à $(-1)^{\frac{1}{2}(m-1)}$, suivant que $P \equiv 1$, ou $P \equiv 3 \pmod{4}$, et que l'on écrive $\left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\dots$ à la place de $\left(\frac{m}{P}\right)$, et $(-1)^{\frac{1}{2}(m-1)}$ à la place de $\left(\frac{2}{m}\right)$, on aura ces résultats :

$$\begin{aligned}
 D = PS^2, & \begin{cases} P \equiv 1 \pmod{4}, & \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right) \dots = 1, \\ P \equiv 3 \pmod{4}, & (-1)^{\frac{1}{2}(m-1)}\left(\frac{m}{p}\right)\left(\frac{m}{p'}\right) \dots = 1, \end{cases} \\
 D = 2PS^2, & \begin{cases} P \equiv 1 \pmod{4}, & (-1)^{\frac{1}{2}(m^2-1)}\left(\frac{m}{p}\right)\left(\frac{m}{p'}\right) \dots = 1, \\ P \equiv 3 \pmod{4}, & (-1)^{\frac{1}{2}(m-1)+\frac{1}{2}(m^2-1)}\left(\frac{m}{p}\right)\left(\frac{m}{p'}\right) \dots = 1. \end{cases}
 \end{aligned}$$

Quant aux caractères particuliers qui n'entrent pas dans ces relations, il n'existe aucune condition à leur égard, ou pour parler plus exactement et pour ne pas aller au delà de ce qui a été démontré, il ne résulte aucune condition qui les concerne, des théorèmes (2) §. 2 dont nous venons de faire usage. Au moyen des résultats précédents et des théorèmes énoncés plus haut, il sera facile de former le tableau suivant qui pourra servir dans chaque cas à faire l'énumération complète des genres différents qui répondent au déterminant D , et dans lequel:

$$r, r', r'', \dots$$

désignent les nombres premiers impairs inégaux qui divisent D sans diviser P .

Premier cas. $D = PS^2, P \equiv 1 \pmod{4}$.

$$\begin{aligned}
 S \equiv 1 \pmod{2}, & \left(\left(\frac{m}{p}\right), \left(\frac{m}{p'}\right), \dots \right) \left(\left(\frac{m}{r}\right), \left(\frac{m}{r'}\right), \dots \right) \\
 S \equiv 2 \pmod{4}, & \left(\left(\frac{m}{p}\right), \left(\frac{m}{p'}\right), \dots \right) (-1)^{\frac{1}{2}(m-1)} \left(\left(\frac{m}{r}\right), \left(\frac{m}{r'}\right), \dots \right) \\
 S \equiv 0 \pmod{4}, & \left(\left(\frac{m}{p}\right), \left(\frac{m}{p'}\right), \dots \right) (-1)^{\frac{1}{2}(m-1)} (-1)^{\frac{1}{2}(m^2-1)} \left(\left(\frac{m}{r}\right), \left(\frac{m}{r'}\right), \dots \right)
 \end{aligned}$$

Second cas. $D = PS^2, P \equiv 3 \pmod{4}$.

$$\begin{aligned}
 S \equiv 1 \pmod{2}, & (-1)^{\frac{1}{2}(m-1)} \left(\left(\frac{m}{p}\right), \left(\frac{m}{p'}\right), \dots \right) \left(\left(\frac{m}{r}\right), \left(\frac{m}{r'}\right), \dots \right) \\
 S \equiv 2 \pmod{4}, & (-1)^{\frac{1}{2}(m-1)} \left(\left(\frac{m}{p}\right), \left(\frac{m}{p'}\right), \dots \right) \left(\left(\frac{m}{r}\right), \left(\frac{m}{r'}\right), \dots \right) \\
 S \equiv 0 \pmod{4}, & (-1)^{\frac{1}{2}(m-1)} \left(\left(\frac{m}{p}\right), \left(\frac{m}{p'}\right), \dots \right) (-1)^{\frac{1}{2}(m^2-1)} \left(\left(\frac{m}{r}\right), \left(\frac{m}{r'}\right), \dots \right)
 \end{aligned}$$

Troisième cas. $D = 2PS^2, P \equiv 1 \pmod{4}$.

$$\begin{aligned}
 S \equiv 1 \pmod{2}, & (-1)^{\frac{1}{2}(m^2-1)} \left(\left(\frac{m}{p}\right), \left(\frac{m}{p'}\right), \dots \right) \left(\left(\frac{m}{r}\right), \left(\frac{m}{r'}\right), \dots \right) \\
 S \equiv 0 \pmod{2}, & (-1)^{\frac{1}{2}(m^2-1)} \left(\left(\frac{m}{p}\right), \left(\frac{m}{p'}\right), \dots \right) (-1)^{\frac{1}{2}(m-1)} \left(\left(\frac{m}{r}\right), \left(\frac{m}{r'}\right), \dots \right)
 \end{aligned}$$

Quatrième cas. $D = 2PS^2$, $P \equiv 3 \pmod{4}$.

$$\begin{aligned} S \equiv 1 \pmod{2}, & \left| \begin{array}{cccc} (-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)}, & \left(\frac{m}{p}\right), & \left(\frac{m}{p'}\right), & \dots \\ (-1)^{\frac{1}{2}(m-1)}, & \left(\frac{m}{p}\right), & \left(\frac{m}{p'}\right), & \dots \end{array} \right| \left(\frac{m}{r}\right), \left(\frac{m}{r'}\right), \dots \\ S \equiv 0 \pmod{2}, & \left| \begin{array}{cccc} (-1)^{\frac{1}{2}(m-1)}, & \left(\frac{m}{p}\right), & \left(\frac{m}{p'}\right), & \dots \\ (-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)}, & \left(\frac{m}{p}\right), & \left(\frac{m}{p'}\right), & \dots \end{array} \right| \left(\frac{m}{r}\right), \left(\frac{m}{r'}\right), \dots \end{aligned}$$

Pour énumérer les caractères complets, c'est-à-dire les genres différents pouvant avoir lieu pour un déterminant donné, il faudra écrire toutes les expressions qui forment la ligne horizontale relative au déterminant donné dans ce tableau, les unes à la suite des autres, après avoir égalé chaque expression à ± 1 , et varier ensuite les signes ambigus de toutes les manières possibles, en s'assujettissant toutefois à la condition que les seconds membres de celles de ces équations qui répondent à la première partie de la ligne horizontale, doivent donner 1 pour produit, cette condition coïncidant avec celle dont la nécessité a été établie plus haut. Soit, par exemple, $D = 2 \cdot 3 \cdot 5^2$. Ce déterminant se rapportant à la première subdivision du quatrième cas, on aura ces 4 caractères complets:

$$\begin{aligned} (-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)} = 1, & \quad \left(\frac{m}{3}\right) = 1, \quad \left(\frac{m}{5}\right) = 1; & (-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)} = 1, & \quad \left(\frac{m}{3}\right) = 1, \quad \left(\frac{m}{5}\right) = -1; \\ (-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)} = -1, & \quad \left(\frac{m}{3}\right) = -1, \quad \left(\frac{m}{5}\right) = 1; & (-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)} = -1, & \quad \left(\frac{m}{3}\right) = -1, \quad \left(\frac{m}{5}\right) = -1. \end{aligned}$$

Suivant la notation de M. GAUSS, ces genres seraient caractérisés comme il suit:

$$\begin{aligned} 1 \text{ et } 3, 8: R3; R5: & \quad 1 \text{ et } 3, 8; R3; N5; \\ 5 \text{ et } 7, 8: N3; R5: & \quad 5 \text{ et } 7, 8; N3; N5. \end{aligned}$$

Il importe de remarquer que les considérations précédentes ne prouvent nullement que les genres compatibles avec la condition énoncée, existent réellement: on peut en conclure seulement qu'il ne saurait y en avoir d'autres. Quant à la question de savoir 1°. si pour chaque déterminant il y a réellement des formes qui appartiennent à chacun des genres ainsi énumérés, et 2°. de quelle manière les formes différentes se distribuent entre les genres, qui ont une existence réelle, c'est une question très difficile qui forme l'un des principaux objets de la seconde partie de la 5^{ième} section de l'ouvrage de M. GAUSS, et dont nous donnerons aussi plus bas la solution au moyen de nos principes.

Nous ferons encore observer, avant d'aller plus loin, que si l'on désigne par λ le nombre des expressions contenues dans la même ligne horizontale du tableau précédent, le nombre des genres énumérés de la manière indiquée sera

évidemment exprimé par 2^{i-1} . Il n'y a qu'une seule exception à cette règle générale, exception qui a lieu lorsque la première partie de la ligne qui est assujettie à une condition dont l'effet est de réduire le nombre des combinaisons de moitié, n'existe pas. En jetant les yeux sur le tableau, on voit de suite que cela ne peut arriver que lorsque le déterminant se trouve compris dans le premier cas, et qu'en même temps P ne contient aucun facteur premier p, p', \dots . Comme l'on a alors d'une part $P \equiv 1 \pmod{4}$ et de l'autre $P = \pm 1$, et par suite $P = 1$, on voit que ce cas n'a lieu que lorsque le déterminant est un carré positif, et que le nombre des genres est alors égal à 2^i .

Tout ce qui précède, est relatif aux formes proprement primitives. Il nous reste à considérer le cas des formes appartenant à l'ordre improprement primitif, et qui ne peuvent représenter que des nombres pairs. Ce cas ne peut avoir lieu que lorsqu'on a $D \equiv 1 \pmod{4}$, et par suite $P \equiv 1 \pmod{4}$, $S \equiv 1 \pmod{2}$. Si l'on désigne par m un entier positif, impair et premier à D , dont le double puisse être exprimé par une pareille forme, on formera sans peine le tableau qui suit, et dont l'usage est entièrement semblable à celui du tableau donné plus haut:

$$D = PS^2, \quad P \equiv 1 \pmod{4}, \quad S \equiv 1 \pmod{2},$$

$$\left(\frac{m}{p}\right), \left(\frac{m}{p'}\right), \dots \parallel \left(\frac{m}{r}\right), \left(\frac{m}{r'}\right), \dots$$

§. 4.

Nous avons maintenant à examiner sous quelles conditions et de combien de manières différentes un nombre m que je suppose positif, impair et premier à D , ou son double, peut être représenté par les formes du déterminant D , en supposant que les valeurs positives ou négatives que l'on attribuera à cet effet aux indéterminées x et y , doivent être premières entre elles. Pour qu'une telle représentation soit possible, il faut que D soit résidu quadratique relativement à m ou à $2m$ (Disq. arithm. 154), conditions dont la seconde ne diffère pas de la première. Or, pour que D soit résidu quadratique par rapport à m , il faut et il suffit qu'on ait pour chacun des diviseurs simples f de m (art. 105):

$$(1) \quad \left(\frac{D}{f}\right) = 1.$$

En supposant f positif, et distinguant comme dans le paragraphe précédent, les

quatre cas suivants que le déterminant D peut présenter:

$$D = PS^2, \quad P \equiv 1 \text{ ou } 3 \pmod{4}, \quad D = 2PS^2, \quad P \equiv 1 \text{ ou } 3 \pmod{4},$$

la condition dont il s'agit, pourra être remplacée, en vertu des théorèmes (2) §. 2 et selon les quatre cas, par l'une de celles-ci:

$$(2) \left(\frac{f}{P}\right) = 1, \quad (-1)^{\frac{1}{2}(f-1)} \left(\frac{f}{P}\right) = 1, \quad (-1)^{\frac{1}{2}(f-1)} \left(\frac{f}{P}\right) = 1, \quad (-1)^{\frac{1}{2}(f-1) + \frac{1}{2}(f'-1)} \left(\frac{f}{P}\right) = 1.$$

Cela posé, soit:

$$(3) \quad ax^2 + 2bxy + cy^2, \quad a'x^2 + 2b'xy + c'y^2, \quad \dots$$

le système complet des formes différentes (proprement primitives) ayant pour déterminant le nombre négatif D , et voyons combien de fois le nombre m dont tout diviseur simple f est supposé satisfaire à la condition (1), peut être représenté de la manière indiquée, par la totalité de ces formes. Si nous désignons par μ le nombre des diviseurs premiers inégaux f de m , la congruence:

$$z^2 \equiv D \pmod{m}$$

aura autant de racines différentes qu'il y aura d'unités dans la puissance 2^μ (art. 105). Soient:

$$l, \quad l', \quad l'', \quad \dots$$

ces racines et cherchons, d'après les préceptes de l'art. 180, les représentations qui appartiennent à chacune de ces racines. Pour obtenir celles qui se rapportent à $z = l$, il faudra voir si parmi les formes (3) il y en a une qui soit équivalente à celle-ci:

$$mx^2 + 2lxy + \frac{l^2 - D}{m} y^2.$$

Or, m étant impair et premier à D , cette dernière sera proprement primitive, et aura donc toujours son équivalente dans le système (3), par laquelle m pourra être représenté de deux manières. Le même raisonnement pouvant s'appliquer à toutes les autres racines l', l'', \dots , on voit que m peut être représenté par la totalité des formes (3) d'autant de manières différentes qu'il y a d'unités dans la puissance $2^{\mu+1}$, deux représentations étant considérées comme différentes lorsqu'elles se font par des formes différentes ou lorsqu'ayant lieu par la même forme, et désignant par x, y et par x', y' les valeurs simultanées des indéterminées, on n'a pas à la fois $x = x'$, et $y = y'$.

Si le système complet (3) est celui de l'ordre improprement primitif, et si en même temps le nombre qu'il s'agit de représenter par ces formes, est

$2m$, on arrive à la même conclusion. Il suffit de remarquer que le nombre des racines de la congruence $z^2 \equiv D \pmod{2m}$ est également 2^μ , et que l'une quelconque de ces racines étant désignée par l , la forme:

$$2m.x^2 + 2l.xy + \frac{l^2 - D}{2m} . y^2$$

sera improprement primitive. C'est ce qui résulte de ce que m est impair et premier à D , et de ce que, l^2 et D étant de la forme $4r+1$, le coefficient de y^2 est pair. Nous avons donc ce théorème dans lequel les deux cas sont réunis dans le même énoncé:

Théorème I.

Soient:

$$a.x^2 + 2b.xy + c.y^2, \quad a'.x^2 + 2b'.xy + c'.y^2, \quad \dots$$

les formes proprement (improprement) primitives différentes, ayant l'entier négatif D pour déterminant; soit encore m un nombre positif, impair et premier à D , dont tous les diviseurs simples f satisfont à celle des conditions (2), qui se rapporte au nombre donné D , et désignons par μ le nombre des facteurs simples inégaux de m . Cela posé, je dis que, si les indéterminées x et y sont assujetties à n'avoir pas de diviseur commun, l'entier m ($2m$) sera toujours représenté par la totalité de ces formes, d'autant de manières différentes qu'il y a d'unités dans la puissance $2^{\mu+1}$.

Remarque. Le théorème précédent est sujet à deux exceptions, dont la première a lieu lorsqu'on a $D = -1$, la seconde lorsqu'on a $D = -3$, et qu'il s'agit des formes de l'ordre improprement primitif. Il résulte de l'article déjà cité de l'ouvrage de M. GAUSS, que le nombre des représentations est respectivement dans ces cas $2^{\mu+2}$ ou $3.2^{\mu+1}$.

Pour établir le théorème que nous allons énoncer, et qui se rapporte au cas où D est un nombre positif (*non-carré*)*, il n'y aura rien à changer aux considérations précédentes, si ce n'est qu'au lieu de s'appuyer sur l'art. 180 des Disq. arithm., il faudra recourir à l'art. 205 du même ouvrage. Pour réunir le cas des formes proprement primitives et celui des formes improprement primitives dans un énoncé commun, nous avons fait usage de la lettre ω , par laquelle il faut entendre le nombre 1 ou 2 selon ces deux cas.

* Les formes dont le déterminant est un carré positif, et qui se décomposent toujours en deux facteurs linéaires, ne sont pas de véritables formes quadratiques. Par cette raison nous les excluons toujours dans ce qui va suivre.

Théorème II.

Soient:

$$ax^2+2bxy+cy^2, \quad a'x^2+2b'xy+c'y^2, \quad \dots$$

les formes proprement (improprement) primitives différentes ayant l'entier positif D pour déterminant; soit encore m un nombre positif, impair et premier à D , dont tous les facteurs simples f satisfont à celle des conditions (2) qui se rapporte au nombre donné D , et désignons par ω le nombre des facteurs simples inégaux de m . Cela posé, et les indéterminées x et y étant assujetties à n'avoir pas de diviseur commun, je dis que les représentations de ωm par la totalité de ces formes pourront toujours être distribuées en 2^ω groupes distincts, en comprenant dans un même groupe deux représentations telles que:

$$ax^2+2bxy+cy^2 = \omega m, \quad a'x'^2+2b'x'y'+c'y'^2 = \omega m,$$

qui se font par la même forme quadratique, et dans lesquelles les valeurs x, y et x', y' des indéterminées sont liées entre elles par les équations:

$$x = \frac{1}{\omega} (x't - (bx' + cy')u), \quad y = \frac{1}{\omega} (y't + (a'x' + b'y')u),$$

t et u désignant des entiers quelconques positifs ou négatifs tels qu'on ait:

$$(4) \quad t^2 - Du^2 = \omega^2.$$

[On peut remarquer que cet énoncé, si l'on y supprimait la condition que D doit être positif, resterait exact et comprendrait alors le théorème I avec ses deux exceptions. En effet, D étant supposé négatif, l'équation (4) n'a en général que ces deux solutions $t = \pm \omega, u = 0$, ce qui donne deux représentations pour chaque groupe, de sorte que le nombre total des représentations, fini dans ce cas, devient $2^{\omega+1}$ comme dans le théorème I. Il n'y a exception que lorsqu'on a ou $D = -1, \omega = 1$; ou $D = -3, \omega = 2$, auxquels cas le nombre des solutions de l'équation (4) est respectivement 4 ou 6, ce qui s'accorde avec les exceptions indiquées plus haut. Mais tout en faisant remarquer ce que le cas de D positif et celui de D négatif ont de commun, comme sous d'autres rapports ces deux cas sont très différents et doivent être traités séparément, nous avons cru devoir donner deux énoncés distincts, pour pouvoir appliquer plus facilement les résultats précédents que nous aurons souvent à employer.]

Il est facile de voir que les représentations, ou ce qui est la même chose,

les solutions de l'équation:

$$(5) \quad ax^2 + 2bxy + cy^2 = om,$$

qui appartiennent au même groupe, peuvent toujours se déduire toutes de l'une quelconque d'entre elles, $x = \alpha$, $y = \gamma$, au moyen des formules:

$$(6) \quad x = \frac{1}{\omega} (\alpha t - (b\alpha + c\gamma)u), \quad y = \frac{1}{\omega} (\gamma t + (a\alpha + b\gamma)u),$$

en attribuant à t et u toutes les valeurs entières, tant positives que négatives, qui satisfont à l'équation (4).

Nous allons faire voir maintenant qu'il existe certaines limites très simples entre lesquelles se trouve toujours comprise une de ces solutions en nombre infini, et entre lesquelles il ne saurait y en avoir plus d'une. Pour éviter des distinctions inutiles à notre objet, nous supposons que dans chacune des formes données:

$$ax^2 + 2bxy + cy^2, \quad a'x^2 + 2b'xy + c'y^2, \quad \dots$$

les coefficients de x^2 et de xy sont positifs, et que celui de y^2 est négatif. On s'assure facilement de la légitimité de cette supposition: il suffit de remarquer que parmi les formes qui composent une même classe, et entre lesquelles nous pouvons en choisir une à volonté, pour construire ce que nous avons appelé le système complet des formes différentes, il y en a toujours au moins une qui satisfait aux conditions énoncées. En effet, la période des formes réduites qui appartiennent à une classe donnée de déterminant positif, contient toujours au moins deux formes (Disq. arithm. art. 187), et il est évident que sur deux formes contiguës quelconques de cette période, il y en a toujours une qui est telle que:

$$(7) \quad a > 0, \quad b > 0, \quad c < 0.$$

Ces conditions ayant lieu, il est facile de voir que parmi les solutions de l'équation (5), il ne saurait y en avoir aucune pour laquelle x soit zéro, puisqu'il résulterait de cette supposition: $cy^2 = om$, ce qui est impossible, c et m ayant des signes opposés. La valeur particulière α sera donc aussi différente de zéro, et nous remarquerons que cette valeur peut toujours être supposée positive. Cela résulte de ce que la solution $x = \alpha$, $y = \gamma$, qui sert de point de départ pour obtenir toutes celles qui appartiennent à un même groupe, peut être choisie à volonté dans ce groupe, et de ce que le groupe qui contient la solution $x = \alpha$, $y = \gamma$, renferme évidemment aussi celle-ci: $x = -\alpha$, $y = -\gamma$, cette dernière se déduisant par les formules (6) de la première, en supposant $t = -\omega$, $u = 0$.

Les solutions, en nombre infini, qui forment un même groupe, et qui résultent des équations (6), peuvent se distribuer en deux groupes partiels dont le premier comprend toutes celles pour lesquelles on a $x > 0$, tandis que celles du second satisfont à la condition $x < 0$.

Nous allons maintenant faire voir que dans le premier de ces groupes partiels, les valeurs de y s'étendent depuis $-\infty$ jusqu'à ∞ , sans que cette indéterminée puisse obtenir la même valeur dans deux solutions différentes, et que celle de ces solutions pour laquelle y a la plus petite valeur positive, différente de zéro, satisfait à des conditions d'inégalité très simples au moyen desquelles il est facile de la séparer de toutes les autres, et de réduire chaque groupe à une représentation unique, ce qui rendra le théorème II entièrement semblable au théorème I qui se rapporte aux déterminants négatifs. Pour remplir l'objet que nous avons en vue, nous observerons qu'il résulte de l'équation:

$$at^2 + 2bct + ct^2 = \omega m,$$

mise sous la forme:

$$(bt + ct)^2 - Da^2 = \omega cm,$$

et de ce que ωcm est négatif, qu'on a, abstraction faite des signes:

$$a \sqrt{D} > bt + ct,$$

et comme on a pareillement en vertu de l'équation (4):

$$\frac{t}{\omega} > \frac{u}{\omega} \sqrt{D},$$

on conclut, en faisant toujours abstraction des signes:

$$at > (bt + ct)u.$$

Il suit de là et de la supposition $a > 0$, que pour embrasser toutes les représentations contenues dans les équations (6) pour lesquelles x a une valeur positive, on n'aura à faire usage que de celles des solutions de l'équation (4) dans lesquelles t a le signe plus. Or, il résulte d'un théorème connu que toutes les solutions qui remplissent cette condition, sont données par les formules:

$$t_n = \frac{\omega}{2} \left\{ \left(\frac{T}{\omega} + \frac{U}{\omega} \sqrt{D} \right)^n + \left(\frac{T}{\omega} - \frac{U}{\omega} \sqrt{D} \right)^n \right\},$$

$$u_n = \frac{\omega}{2\sqrt{D}} \left\{ \left(\frac{T}{\omega} + \frac{U}{\omega} \sqrt{D} \right)^n - \left(\frac{T}{\omega} - \frac{U}{\omega} \sqrt{D} \right)^n \right\},$$

dans lesquelles T et U désignent les plus petits nombres positifs (autres que

ω et 0) qui satisfont à l'équation (4), n devant être égalé successivement à tous les entiers depuis $-\infty$ jusqu'à ∞ . On aura donc pour le groupe partiel dans lequel x est positif, en distinguant les différentes solutions de ce groupe par l'indice n , déjà employé dans les équations précédentes:

$$x_n = \frac{1}{\omega} (a t_n - (ab + \gamma c) u_n), \quad y_n = \frac{1}{\omega} (\gamma t_n + (aa + \gamma b) u_n).$$

En substituant les expressions de t_n , u_n , la seconde de ces équations deviendra:

$$y_n = \left(\frac{\gamma \sqrt{D} + aa + \gamma b}{2\sqrt{D}} \right) \left(\frac{T}{\omega} + \frac{U}{\omega} \sqrt{D} \right)^n + \left(\frac{\gamma \sqrt{D} - aa - \gamma b}{2\sqrt{D}} \right) \left(\frac{T}{\omega} - \frac{U}{\omega} \sqrt{D} \right)^n.$$

Il est facile de voir que les quantités:

$$\gamma \sqrt{D} + aa + \gamma b, \quad \gamma \sqrt{D} - aa - \gamma b$$

sont la première positive, la seconde négative. Pour s'en assurer il suffira de faire voir que $aa + \gamma b$ est numériquement supérieur à $\gamma \sqrt{D}$ et positif. La première de ces assertions se prouve, en mettant l'équation:

$$aa^2 + 2ba\gamma + c\gamma^2 = \omega m$$

sous la forme:

$$(aa + \gamma b)^2 - D\gamma^2 = \omega am.$$

et observant que le second membre est positif. Pour justifier la seconde assertion, on remarquera que, puisque la valeur numérique de $aa + \gamma b$ surpasse celle de $\gamma \sqrt{D}$, elle surpassera *a fortiori* celle de γb , b étant $< \sqrt{D}$. De là et de ce que aa a le signe positif, on conclut que $aa + \gamma b$ est également positif.

Comme en vertu de ce qui précède, les coefficients qui entrent dans l'expression de y_n , sont le premier positif, le second négatif, et que d'un autre côté, les quantités positives:

$$\frac{T}{\omega} + \frac{U}{\omega} \sqrt{D}, \quad \frac{T}{\omega} - \frac{U}{\omega} \sqrt{D},$$

dont le produit est 1, sont évidemment la première supérieure, la seconde inférieure à l'unité, on voit sans peine que chacun des deux termes dont se compose y_n , croît avec l'indice n . On aura donc, quel que soit cet indice:

$$y_n > y_{n-1},$$

ce qui prouve, comme nous l'avons avancé plus haut, que l'indéterminée y ne saurait obtenir deux fois la même valeur dans le groupe partiel où x est positif, et l'on voit également que y doit passer du négatif au positif, car on a

évidemment $y_{-x} = -\infty$, $y_x = \infty$. Pour obtenir la solution que nous avons en vue, et dans laquelle y_n a la plus petite valeur positive, différente de zéro, il faudra poser ces deux conditions:

$$y_n > 0, \quad y_{n-1} < 0.$$

Si l'on observe qu'en vertu des expressions de x_n , y_n , t_n , u_n , données plus haut, on a la relation:

$$y_{n-1} = \frac{1}{\omega} (y_n T - (ax_n + by_n) U),$$

la seconde de ces conditions prendra cette autre forme:

$$(T - bU)y_n < aUx_n.$$

Comme on a $T > \sqrt{VD}$, $b < \sqrt{VD}$, et par suite $T - bU > 0$, l'inégalité précédente est équivalente à celle-ci:

$$y_n < \frac{aU}{T - bU} x_n.$$

Il résulte de ce qui précède, que parmi les représentations en nombre infini, formant un même groupe, et qui sont toutes données par les équations (6), il y en a toujours une qui satisfait à ces trois conditions:

$$(8) \quad x > 0, \quad y > 0, \quad y < \frac{aU}{T - bU} x.$$

Ces inégalités ont été déduites de la définition de la solution particulière que nous voulions séparer de toutes les autres contenues dans le même groupe qu'elle. D'après cette définition, la solution dont il s'agit devait appartenir au premier des deux groupes partiels, et répondre dans ce groupe à la plus petite valeur positive de y . On peut prouver réciproquement que toute solution pour laquelle les inégalités précédentes ont lieu, est nécessairement, parmi toutes les solutions formant avec elle un même groupe total, celle à laquelle s'applique la définition précédente: il suffit pour cela de répéter en sens inverse les raisonnements que nous venons de développer. Cela étant, on voit que le théorème II peut être remplacé par un autre théorème dont voici l'énoncé.

Théorème III.

Les suppositions du théorème II étant conservées, si l'on ajoute que les coefficients et les indéterminées de la forme $ax^2 + 2bxy + cy^2$, doivent satisfaire aux conditions (7) et (8), et que l'on assujettisse toutes les autres formes à des

conditions analogues, je dis que le nombre des représentations différentes de l'entier om , que l'on peut effectuer au moyen des formes données, sera exprimé par la puissance 2^u .

Pour rendre plus faciles les applications que nous aurons à faire du théorème précédent, il conviendra de mettre sous une forme géométrique le résultat sur lequel ce théorème est fondé. Soient à cet effet OX , OY deux axes rectangulaires des x et des y , dirigés dans le sens des coordonnées positives, le premier horizontalement, le second verticalement et de bas en haut. Les variables x et y dans l'équation:

$$ax^2 + 2bxy + cy^2 = om$$

étant considérées comme continues, cette équation sera à une hyperbole, et l'on déduira facilement des conditions $a > 0$, $b > 0$, $c < 0$, que l'axe des y sépare l'une de l'autre, les deux branches infinies de cette courbe. Si donc nous appelons première branche celle de ces deux branches infinies sur laquelle l'abscisse x est partout positive, le premier des deux groupes partiellement distingués, répondra à cette première branche. Cela étant l'interprétation géométrique du résultat établi plus haut consiste en ce que, parmi les solutions en nombre infini formant le même groupe total, et qui sont toutes comprises dans les équations (6), il y en a toujours une, et qu'il ne saurait y en avoir plus d'une, qui soit représentée par un point de l'arc de la première branche, intercepté d'une part par l'axe OX , et de l'autre par la droite qui a pour équation:

$$y = \frac{aU}{T} \frac{1}{bU} x;$$

ce à quoi il faut ajouter qu'on doit toujours exclure la solution qui répond à l'extrémité inférieure de cet arc.

§. 5.

Il nous reste une dernière question préliminaire à résoudre, avant d'en venir au véritable objet de ce mémoire. Cette question consiste à assigner toutes les valeurs simultanées des indéterminées x et y qui, étant substituées dans une forme donnée du déterminant D , rendent cette forme première à D , et en outre impaire ou impairement paire suivant qu'il s'agit d'une forme proprement ou improprement primitive. Nous désignons par D_1 la valeur numérique de D , et nous commencerons cette recherche par l'examen du cas où la forme donnée appartient à l'ordre proprement primitif. Ce cas se subdivise lui-même,

suivant que D est pair ou impair. Soit en premier lieu D impair. Les indéterminées x et y étant mises sous la forme:

$$2D_1r + a, \quad 2D_1w + \gamma.$$

où r, w désignent des entiers quelconques positifs ou négatifs, a, γ étant des nombres pris l'un et l'autre dans la suite:

$$0, 1, 2, \dots, 2D_1 - 1.$$

on aura évidemment:

$$ax^2 + 2bxy + cy^2 \equiv aa^2 + 2bay + c\gamma^2 \pmod{2D_1}.$$

La question proposée revient donc à voir pour lesquelles des combinaisons a, γ , ou plutôt, pour combien de ces combinaisons (car c'est uniquement leur nombre qu'il nous importe de connaître) le second membre est premier à $2D_1$. Nous observerons d'abord qu'on peut, sans nuire en rien à la généralité de la question, supposer l'un des coefficients extrêmes, le premier a par exemple, sans diviseur commun avec $2D_1$. En effet, si cette condition n'a pas lieu dans la forme donnée, on peut toujours transformer celle-ci en une autre où elle se trouve remplie. Soit $a'x^2 + 2b'x'y' + c'y'^2$ la nouvelle forme équivalente à la première, et soient:

$$x = px' + qy', \quad y = rx' + sy', \quad ps - qr = 1$$

les équations qui correspondent à cette transformation. Si maintenant dans les congruences:

$$a \equiv pa' + q\gamma', \quad \gamma \equiv ra' + s\gamma' \pmod{2D_1}$$

on combine les nombres a', γ' , pris l'un et l'autre dans la suite:

$$0, 1, 2, \dots, 2D_1 - 1.$$

de toutes les manières possibles, et que l'on détermine a, γ de manière que ces nombres se trouvent compris entre les mêmes limites, à chaque combinaison a', γ' correspondra une combinaison a, γ , et réciproquement, comme on le voit en mettant les congruences précédentes sous la forme:

$$a' = sa - q\gamma, \quad \gamma' \equiv -ra + p\gamma \pmod{2D_1}.$$

De là et de ce que l'on a évidemment:

$$aa^2 + 2bay + c\gamma^2 \equiv a'a'^2 + 2b'a'\gamma' + c'\gamma'^2 \pmod{2D_1}.$$

on conclut que les nombres des combinaisons a, γ et a', γ' pour lesquelles:

$$aa^2 + 2bay + c\gamma^2 \quad \text{et} \quad a'a'^2 + 2b'a'\gamma' + c'\gamma'^2$$

sont premiers à $2D_1$ coïncident. Cette conclusion justifiant l'assertion avancée

plus haut, nous pouvons considérer a comme premier à $2D_1$. Cela posé, pour que le trinôme:

$$aa^2+2ba\gamma+cy^2$$

n'ait pas de diviseur commun avec $2D_1$, il faut et il suffit que le produit:

$$a(aa^2+2ba\gamma+cy^2) = (aa+by)^2 - D\gamma^2$$

jouisse de la même propriété, et par suite, que $aa+by$ soit premier à $2D_1$, lorsque γ est pair, ou que $aa+by$ soit pair et premier à D_1 , lorsque γ est impair. Or, γ ayant une valeur déterminée, celles de l'expression $aa+by$, lorsqu'on y pose successivement:

$$a = 0, 1, 2, \dots, 2D_1-1. \quad \bullet$$

coïncideront, abstraction faite des multiples de $2D_1$, avec la même suite. Tout se réduit donc à voir dans le cas de γ pair, combien la suite précédente renferme de termes premiers à $2D_1$, et dans le cas de γ impair, combien il y en a dans la même suite, qui jouissent de la double propriété d'être pairs et premiers à D_1 . Si l'on désigne par A le nombre des entiers positifs non-supérieurs*) à D_1 , qui n'ont pas de diviseur commun avec D , le nombre des termes en question sera, pour l'un et l'autre cas, exprimé par A . Comme d'un autre côté, γ est susceptible de $2D_1$ valeurs différentes, on voit que les combinaisons a, γ qui donnent à:

$$aa^2+2ba\gamma+cy^2$$

une valeur première à $2D_1$, sont au nombre de $2D_1A$. Une discussion toute semblable étant appliquée au cas où D est pair, fait voir que le nombre des combinaisons est alors $4D_1A$.

Considérons en dernier lieu le cas où la forme donnée:

$$ax^2+2bxy+cy^2$$

appartient à l'ordre improprement primitif. Si nous posons:

$$\frac{1}{2}a = a', \quad \frac{1}{2}c = c'$$

et comme précédemment:

$$x = 2D_1v+a, \quad y = 2D_1w+\gamma,$$

nous aurons:

$$a'x^2+bxy+c'y^2 \equiv a'a^2+ba\gamma+c'\gamma^2 \pmod{2D_1},$$

*) Je dis à dessein non-supérieurs, pour que le cas de $D_1=1$ ne fasse pas exception.

et il s'agira de voir pour combien de combinaisons α, γ le second membre est impair et premier à D_1 . Pour y parvenir de la manière la plus simple, nous supposons, ce qui est permis, que a' n'ait pas de diviseur commun avec $2D_1$. Cela étant, il faut distinguer le cas où l'on a $D \equiv 1$, et celui où $D \equiv 5 \pmod{8}$. Dans le premier de ces deux cas, b étant impair, il résulte de l'équation:

$$D = b^2 - ac = b^2 - 4a'c',$$

que c' est pair, et l'on voit de même que dans le second, c' est impair. On conclut de là que:

$$a'a^2 + b\alpha\gamma + c'\gamma^2$$

ne saurait être impair dans le premier cas, à moins que les nombres α, γ ne soient le premier impair, le second pair, et dans le second, à moins que α, γ ne soient ou l'un pair, l'autre impair, ou impairs tous les deux. Pour avoir égard à l'autre condition d'après laquelle:

$$a'a^2 + b\alpha\gamma + c'\gamma^2$$

doit être premier à D_1 , on remarquera qu'il faut et qu'il suffit, pour qu'elle soit remplie, que le produit:

$$4a'(a'a^2 + b\alpha\gamma + c'\gamma^2) = (aa + b\gamma)^2 - D\gamma^2$$

jouisse de la même propriété. Cela posé, si nous supposons d'abord $D \equiv 1 \pmod{8}$, il faudra, après avoir attribué à γ une valeur déterminée paire, évaluer α à chaque terme de la suite:

$$1, 3, 5, \dots, 2D_1 - 1,$$

et voir combien de fois $aa + b\gamma$, ou ce qui est la même chose, le reste de cette expression, pris relativement au diviseur D_1 , est premier à D_1 . Or il est facile de voir que les restes de $aa + b\gamma$ sont, abstraction faite de l'ordre:

$$0, 1, 2, \dots, D_1 - 1;$$

on en conclut qu'à chaque valeur de γ correspond un nombre A de valeurs impaires de α , telles que:

$$a'a^2 + b\alpha\gamma + c'\gamma^2$$

soit impair et premier à D . Il résulte de là et de ce que le nombre γ est lui-même susceptible de D_1 valeurs différentes, que le nombre des combinaisons α, γ qui donnent à l'expression:

$$\frac{1}{2}(aa^2 + 2b\alpha\gamma + c\gamma^2)$$

une valeur impaire et première à D , est égal à $D_1 A$. Si nous considérons en

second lieu le cas où $D \equiv 5 \pmod{8}$, on trouve, comme dans le cas précédent, qu'à chaque valeur paire de γ , il correspond un nombre de valeurs convenables de a , égal à \mathcal{A} , puisque, γ étant pair, a doit être impair; mais il n'en est plus de même, lorsque la valeur déterminée que l'on attribue à γ , est impaire, a pouvant être alors pair ou impair. Il faut, dans cette dernière supposition, égaliser a dans l'expression $aa+b\gamma$ à chacun des nombres:

$$0, 1, 2, \dots, 2D_1-1.$$

Or, les valeurs de $aa+b\gamma$, correspondant à ces nombres, étant diminuées des multiples de D_1 qu'elles contiennent, coïncideront évidemment avec la suite:

$$0, 1, 2, \dots, D_1-1,$$

chacun des termes de cette suite étant supposé écrit deux fois. On conclut de là que les valeurs convenables de a , répondant à une valeur impaire donnée de γ , sont toujours au nombre de $2\mathcal{A}$. Si l'on remarque maintenant que, parmi les valeurs:

$$0, 1, 2, \dots, 2D_1-1$$

dont γ est susceptible, il y en a D_1 qui sont paires, et autant qui sont impaires, on verra que dans le cas où l'on a $D \equiv 5 \pmod{8}$, le nombre des combinaisons a, γ , rendant le trinôme:

$$\frac{1}{2}(aa^2+2bay+cy^2)$$

impair et premier à D , est égal à $3D_1\mathcal{A}$.

Nous résumerons ici les résultats qui ont été établis dans ce paragraphe. La valeur numérique du déterminant D étant désignée par D_1 , et \mathcal{A} exprimant le nombre de ceux des termes:

$$1, 2, \dots, D_1$$

qui n'ont pas de diviseur commun avec D_1 , les valeurs simultanées de x et de y qui rendent une forme quelconque de ce déterminant, ou la moitié de cette forme lorsqu'elle appartient à l'ordre improprement primitif, impaire et première à D , peuvent toujours se distribuer en systèmes de la forme:

$$x = 2D_1v + a, \quad y = 2D_1w + \gamma,$$

où v et w désignent des entiers indéterminés positifs ou négatifs, et où a et γ sont l'un et l'autre compris dans la suite:

$$0, 1, 2, \dots, 2D_1-1:$$

quant au nombre des systèmes qui jouissent de la propriété énoncée, il sera, lorsqu'il s'agit d'une forme proprement primitive $2D_1\mathcal{A}$ ou $4D_1\mathcal{A}$, suivant que

D est impair ou pair, et lorsque la forme est improprement primitive, $D_1 \Delta$ ou $3D_1 \Delta$, suivant que l'on a $D \equiv 1$ ou $D \equiv 5 \pmod{8}$.

Nous terminerons les préliminaires en démontrant le lemme qui suit. „Soit $K = kk'k'' \dots$ le produit des nombres premiers positifs, impairs et inégaux k, k', k'', \dots , et désignons par L un entier quelconque qui divise K . Posons encore $\theta = \pm 1$, $\eta = \pm 1$, les signes ambigus étant quelconques et indépendants l'un de l'autre. Cela étant, je dis que l'expression:

$$\Sigma \theta^{1(n-1)} \eta^{\frac{1}{8}(n^2-1)} \left(\frac{n}{L}\right),$$

où le signe sommatoire s'étend à tous les entiers n premiers à $2K$, et compris depuis $n = 1$ jusqu'à $n = 8K - 1$, est toujours égale à zéro, si on n'a pas simultanément $\theta = 1$, $\eta = 1$, $L = 1$.“

Désignons par a l'un quelconque des nombres $1, 2, \dots, k-1$, par a' l'un quelconque des nombres $1, 2, \dots, k'-1$, et ainsi de suite. Soit encore b l'un quelconque des nombres $1, 3, 5, 7$. Cela posé, il est facile de voir que l'on obtiendra toutes les valeurs que n doit recevoir dans la somme précédente, en déterminant, pour chacune des combinaisons a, a', \dots, b , le nombre n , moindre que $8K$, qui satisfait aux congruences simultanées:

$$n \equiv a \pmod{k}, \quad n \equiv a' \pmod{k'}, \quad \dots, \quad n \equiv b \pmod{8}.$$

On conclut de ces congruences:

$$\left(\frac{n}{k}\right) = \left(\frac{a}{k}\right), \quad \left(\frac{n}{k'}\right) = \left(\frac{a'}{k'}\right), \quad \dots, \quad \theta^{1(n-1)} = \theta^{1(b-1)}, \quad \eta^{\frac{1}{8}(n^2-1)} = \eta^{\frac{1}{8}(b^2-1)}.$$

Si maintenant on désigne ceux des nombres premiers k, k', \dots qui sont contenus dans L , par k_0, k'_0, \dots les autres par k_1, k'_1, \dots la somme du lemme:

$$\Sigma \theta^{1(n-1)} \eta^{\frac{1}{8}(n^2-1)} \left(\frac{n}{L}\right) \quad \text{ou} \quad \Sigma \theta^{1(n-1)} \eta^{\frac{1}{8}(n^2-1)} \left(\frac{n}{k_0}\right) \left(\frac{n}{k'_0}\right) \dots,$$

sera exprimé par le produit*):

$$(k_1-1)(k'_1-1) \dots \Sigma_a \left(\frac{a}{k_0}\right) \Sigma_{a'} \left(\frac{a'}{k'_0}\right) \dots \Sigma_b \theta^{1(b-1)} \eta^{\frac{1}{8}(b^2-1)}$$

$(a = 1, 2, \dots, k_0-1; \quad a' = 1, 2, \dots, k'_0-1; \quad \dots; \quad b = 1, 3, 5, 7)$

dont les facteurs:

$$\Sigma_a \left(\frac{a}{k_0}\right), \quad \Sigma_{a'} \left(\frac{a'}{k'_0}\right), \quad \dots$$

s'évanouissent évidemment. Comme on a encore:

$$\Sigma_b \theta^{1(b-1)} \eta^{\frac{1}{8}(b^2-1)} = 0$$

*) Im Originaltext sind die einzelnen Factoren des Products angegeben; die Formel-Darstellung habe ich der Deutlichkeit wegen hinzugefügt und deshalb noch einige Aenderungen angebracht. K.

pour les trois cas: $\theta = 1, \eta = -1$; $\theta = -1, \eta = 1$; $\theta = -1, \eta = -1$, il résulte que l'expression:

$$\Sigma \theta^{l(n-1)} \eta^{\frac{1}{2}l(n-1)} \binom{n}{L}$$

s'évanouit toujours, à moins qu'on n'ait à la fois $\theta = 1, \eta = 1, L = 1$, ce qu'il s'agissait de prouver.

§. 6.

En passant maintenant aux questions indiquées dans le préambule de ce mémoire, nous conserverons les notations dont nous avons fait usage dans les §§. 3, 4 et 5. Nous poserons donc:

$$(1) \quad D = PS^2, \quad \text{ou} \quad D = 2PS^2,$$

S^2 étant toujours le plus grand carré qui divise D , et:

$$(2) \quad P = pp'p'' \dots,$$

p, p', p'', \dots étant des nombres premiers impairs, positifs ou négatifs, tous différents les uns des autres. Nous poserons aussi:

$$(3) \quad R = rr'r'' \dots,$$

r, r', r'', \dots désignant, comme plus haut, les facteurs premiers impairs inégaux, contenus dans S , sans l'être dans P . Soit encore q un nombre premier positif impair quelconque, qui n'est contenu ni dans P ni dans R , et décomposons chacun de ces produits d'une manière quelconque en deux facteurs, sans exclure le cas où l'un de ces facteurs serait égal à l'unité, c'est-à-dire, écrivons les deux équations:

$$(4) \quad P = P_1 P_2, \quad R = R_1 R_2.$$

Posons enfin:

$$(5) \quad \delta = \pm 1, \quad \varepsilon = \pm 1, \quad \theta = \pm 1, \quad \eta = \pm 1.$$

les signes étant quelconques et indépendants les uns des autres. Cela étant et s désignant une variable continue positive, assujettie à rester supérieure à l'unité, nous aurons par le développement en série, et en ayant égard aux équations (2) et (3) du §. 2:

$$\frac{1}{1 - \theta^{\delta(q-1)} \eta^{\frac{1}{2}\delta(q-1)} \left(\frac{q}{P_2 R_1} \right) \frac{1}{q^s}} = 1 + \dots + \theta^{\delta(q^l-1)} \eta^{\frac{1}{2}\delta(q^l-1)} \left(\frac{q^l}{P_2 R_1} \right) \frac{1}{(q^s)^s} + \dots,$$

où, pour abrégér, on n'a écrit dans le second membre que son terme général, dans lequel il faut égarder l successivement à toutes les valeurs entières depuis $l = 0$ jusqu'à $l = \infty$.

Supposons maintenant que dans l'équation précédente, on mette pour q toutes les valeurs dont ce nombre est susceptible, c'est-à-dire tous les nombres premiers impairs positifs qui ne divisent pas D , et que l'on forme le produit de toutes ces équations. Le produit des seconds membres formera une série dont la loi est très facile à reconnaître, si l'on se rappelle que, d'après un théorème connu, un nombre composé ne peut résulter que d'une seule manière, de la multiplication de facteurs simples, et que l'on continue en même temps à avoir égard aux théorèmes cités du §. 2. On obtient ainsi l'équation:

$$(6) \quad \Pi \frac{1}{1 - \theta^{\frac{1}{2}(q-1)} \eta^{\frac{1}{2}(q^2-1)} \left(\frac{q}{P_2 R_1} \right) \frac{1}{q}} = \Sigma \theta^{\frac{1}{2}(n-1)} \eta^{\frac{1}{2}(n^2-1)} \left(\frac{n}{P_2 R_1} \right) \frac{1}{n^s},$$

le signe de multiplication Π se rapportant à toutes les valeurs de q , précédemment définies, et le signe sommatoire s'étendant à tous les entiers, compris depuis $n = 1$ jusqu'à $n = \infty$, qui remplissent la double condition d'être impairs et premiers à D , ou plus simplement, qui sont premiers à $2D$.

Avant d'aller plus loin, nous aurions à montrer la nécessité de la supposition faite plus haut, et d'après laquelle on doit avoir $s > 1$. On s'en rendra facilement compte, si l'on remarque que la série précédente n'a une somme indépendante de l'arrangement de ses termes, que lorsque la condition $s > 1$ a lieu, et qu'il en est de même du produit, dont la valeur n'est également indépendante de l'ordre de ses facteurs qu'autant que la même condition est remplie. Il me semble d'autant plus inutile d'entrer dans de plus grands développements à ce sujet, que je me suis déjà expliqué avec détail sur le point en question, dans la démonstration du théorème sur la progression arithmétique que j'ai citée plus haut et qui est fondée sur une équation de même nature, mais plus générale que la précédente.

Si dans l'équation (6) on remplace θ , η respectivement par $\delta\theta$, $\varepsilon\eta$, et que l'on change en même temps P_2 en P_1 , elle deviendra:

$$(7) \quad \Pi \frac{1}{1 - (\delta\theta)^{\frac{1}{2}(q-1)} (\varepsilon\eta)^{\frac{1}{2}(q^2-1)} \left(\frac{q}{P_1 R_1} \right) \frac{1}{q}} = \Sigma (\delta\theta)^{\frac{1}{2}(n-1)} (\varepsilon\eta)^{\frac{1}{2}(n^2-1)} \left(\frac{n}{P_1 R_1} \right) \frac{1}{n^s}.$$

On a encore, en y faisant $\theta = 1$, $\eta = 1$, $P_2 = 1$, $R_1 = 1$, et remplaçant s par $2s$:

$$(8) \quad \Pi \frac{1}{1 - \frac{1}{q^{2s}}} = \Sigma \frac{1}{n^{2s}},$$

les signes de multiplication et de sommation s'étendant toujours aux valeurs de q et de n , précédemment définies. Le produit des équations (6) et (7) étant divisé par l'équation (8), le facteur général dans le premier membre sera :

$$\frac{\left(1 + \frac{1}{q^s}\right)\left(1 + \frac{1}{q^s}\right)}{\left(1 - (\delta\theta)^{\frac{1}{2}(q-1)}(\varepsilon\eta)^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_1 R_1}\right)\frac{1}{q^s}\right)\left(1 - \theta^{\frac{1}{2}(q-1)}\eta^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_2 R_1}\right)\frac{1}{q^s}\right)}$$

Comme le numérateur de cette fraction est évidemment équivalent à :

$$\left(1 + \theta^{\frac{1}{2}(q-1)}\eta^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_2 R_1}\right)\frac{1}{q^s}\right)\left(1 - \theta^{\frac{1}{2}(q-1)}\eta^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_2 R_1}\right)\frac{1}{q^s}\right),$$

elle pourra se mettre sous cette forme plus simple :

$$\frac{1 + \theta^{\frac{1}{2}(q-1)}\eta^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_2 R_1}\right)\frac{1}{q^s}}{1 - (\delta\theta)^{\frac{1}{2}(q-1)}(\varepsilon\eta)^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_1 R_1}\right)\frac{1}{q^s}}$$

L'expression précédente présente deux cas différents, suivant que l'on a :

$$\delta^{\frac{1}{2}(q-1)}\varepsilon^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_1 P_2}\right) = \delta^{\frac{1}{2}(q-1)}\varepsilon^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P}\right) = -1 \text{ ou } +1.$$

Dans le premier de ces deux cas, elle est égale à l'unité et peut être omise dans le produit; dans le second, on peut lui donner cette autre forme :

$$\frac{1 + \theta^{\frac{1}{2}(q-1)}\eta^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_2 R_1}\right)\frac{1}{q^s}}{1 - \theta^{\frac{1}{2}(q-1)}\eta^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P_2 R_1}\right)\frac{1}{q^s}}$$

Les doubles signes dans les valeurs $\delta = \pm 1$, $\varepsilon = \pm 1$, que contient l'équation (7), ont été tout à fait arbitraires jusqu'à présent. Nous supposons désormais que suivant les quatre cas déjà distingués dans les §§. 3 et 4, et que le déterminant D peut présenter, savoir :

$$D = PS^2, \quad P \equiv 1 \text{ ou } 3 \pmod{4}; \quad D = 2PS^2, \quad P \equiv 1 \text{ ou } 3 \pmod{4}.$$

ces signes seront respectivement :

$$(9) \quad \delta = 1, \quad \varepsilon = 1; \quad \delta = -1, \quad \varepsilon = 1; \quad \delta = 1, \quad \varepsilon = -1; \quad \delta = -1, \quad \varepsilon = -1.$$

Cela étant, la condition :

$$\delta^{\frac{1}{2}(q-1)}\varepsilon^{\frac{1}{2}(q^2-1)}\left(\frac{q}{P}\right) = 1$$

coïncidera avec celle des quatre conditions (2) du §. 4 qui correspond à chacun des quatre cas précédents. En désignant donc les nombres premiers q positifs,

impairs et non-diviseurs de D qui y satisfont, par f , cette lettre aura la même signification que dans le §. 4, c'est-à-dire que l'on aura :

$$(10) \quad \delta^{k(f-1)} \varepsilon^{\frac{1}{2}(f^2-1)} \left(\frac{f}{P} \right) = 1,$$

et le premier membre de l'équation dont l'origine a été indiquée plus haut, sera :

$$II \frac{1 + \theta^{k(f-1)} i^{\frac{1}{2}(f^2-1)} \left(\frac{f}{P_2 R_1} \right) \frac{1}{f^s}}{1 - \theta^{k(f-1)} i^{\frac{1}{2}(f^2-1)} \left(\frac{f}{P_2 R_1} \right) \frac{1}{f^s}}.$$

le signe II s'étendant à toutes les valeurs de f . Au moyen de l'équation :

$$\frac{1+z}{1-z} = 1 + 2z + 2z^2 + 2z^3 + \dots$$

et en ayant égard aux équations (2) et (3) du §. 2, le facteur général du produit précédent pourra se développer en une série dont le $(l+1)^{\text{ème}}$ terme est :

$$2\theta^{k(f-1)} i^{\frac{1}{2}(f^2-1)} \left(\frac{f^l}{P_2 R_1} \right) \frac{1}{(f^l)^s}.$$

Le premier terme qui répond à $l=0$, fait exception à cette loi et a l'unité pour valeur. Il est facile de conclure de là, et en ayant toujours égard aux équations citées du §. 2, que le produit précédent peut lui-même prendre la forme d'une série, ayant pour terme général :

$$\theta^{k(m-1)} i^{\frac{1}{2}(m^2-1)} \left(\frac{m}{P_2 R_1} \right) \frac{2^\mu}{m^s},$$

où m désigne généralement tous les entiers positifs, impairs et premiers à D , n'ayant que des diviseurs simples f tels que la condition (10) soit satisfaite, et où μ indique, comme dans le §. 4, le nombre des diviseurs simples inégaux de m , sans compter le diviseur 1. On peut remarquer que le terme qui répond à $m=1$, ne fait pas exception à la loi générale, l'expression précédente se réduisant à l'unité dans ce cas. Nous avons donc l'équation :

$$(11) \quad \left\{ \begin{aligned} & \sum \frac{1}{n^{2s}} \cdot \sum \theta^{k(m-1)} i^{\frac{1}{2}(m^2-1)} \left(\frac{m}{P_2 R_1} \right) \frac{2^\mu}{m^s} \\ & = \sum (\delta\theta)^{\frac{1}{2}(n-1)} (\varepsilon\eta)^{\frac{1}{2}(n^2-1)} \left(\frac{n}{P_1 R_1} \right) \frac{1}{n^s} \cdot \sum \theta^{k(n-1)} i^{\frac{1}{2}(n^2-1)} \left(\frac{n}{P_2 R_1} \right) \frac{1}{n^s}, \end{aligned} \right.$$

dans laquelle on doit étendre les sommations à tous les entiers n ou m , précédemment définis, et l'on doit se rappeler que les valeurs $\delta = \pm 1$, $\varepsilon = \pm 1$ sont celles que nous avons fixées par les conditions (9), tandis que les signes dans les équations $\theta = \pm 1$, $\eta = \pm 1$ restent arbitraires.

En faisant $\theta = 1$, $\eta = 1$, $P_2 = 1$, $R_1 = 1$, et par suite $P_1 = P$, l'équation précédente prendra la forme:

$$(12) \quad \Sigma \frac{1}{n^{2s}} \cdot \Sigma \frac{2^u}{m^s} = \Sigma \frac{1}{n^s} \cdot \Sigma \delta^{s(n-1)} \epsilon^{\frac{1}{2}(n^2-1)} \binom{n}{P} \frac{1}{n^s}.$$

C'est cette équation particulière qui nous servira à déterminer le nombre des formes différentes qui répondent à un déterminant quelconque positif ou négatif. Il faudra, dans cette recherche, traiter séparément le cas où D est positif et celui où D est négatif, et subdiviser encore chacun de ces deux cas suivant qu'il s'agira de formes proprement ou improprement primitives. Mais comme il y a néanmoins une partie commune à l'analyse de ces quatre cas, il conviendra, pour n'avoir pas à présenter deux fois les mêmes considérations, que nous nous occupions d'abord de cette partie de la discussion, dont l'objet consiste à voir quelle forme prend le second membre de l'équation (12), si l'on y suppose $s = 1 + \varrho$, et que l'on considère la variable positive ϱ comme devenant moindre que toute quantité donnée.

Pour commencer cet examen par le premier des deux facteurs contenus dans le second membre, soient e, e', e'', \dots ceux des nombres:

$$1, 2, 3, \dots, 2D_1 - 1$$

qui n'ont pas de diviseur commun avec $2D_1$. Cela posé, il est évident que la somme $\Sigma \frac{1}{n^{1+\varrho}}$, où n ne doit recevoir que des valeurs positives et premières à $2D_1$, peut être décomposée en autant de sommes partielles de la forme:

$$\frac{1}{e^{1+\varrho}} + \frac{1}{(2D_1+e)^{1+\varrho}} + \frac{1}{(4D_1+e)^{1+\varrho}} + \dots$$

qu'il y a de termes dans la suite e, e', e'', \dots . Comme, d'un autre côté, on conclut facilement du résultat obtenu plus haut sur la série (1) du §. 1, que chacune de ces sommes partielles prend la forme $\frac{1}{2D_1} \cdot \frac{1}{\varrho}$, et qu'il est d'ailleurs évident que le nombre de ces sommes partielles, ou ce qui revient au même, le nombre des termes e, e', e'', \dots est \mathcal{A} ou $2\mathcal{A}$, selon que D est impair ou pair, la lettre \mathcal{A} ayant la même signification que dans le §. 5, on aura selon ces deux cas:

$$(13) \quad \Sigma \frac{1}{n^{1+\varrho}} = \frac{\mathcal{A}}{2D_1} \cdot \frac{1}{\varrho}, \quad \text{ou} \quad \Sigma \frac{1}{n^{1+\varrho}} = \frac{\mathcal{A}}{D_1} \cdot \frac{1}{\varrho},$$

la variable ϱ étant toujours supposée infiniment petite. Si nous considérons

en second lieu l'autre facteur du second membre, il est facile de voir que ce facteur est un cas particulier de la série à laquelle se rapporte le troisième des lemmes du §. 1; il faudra, pour l'y comprendre, supposer dans la série générale de ce lemme:

$$c_n = \delta^{\frac{1}{2}(n-1)} \varepsilon^{\frac{1}{2}(n^2-1)} \binom{n}{P}, \quad \text{ou } c_n = 0,$$

suivant que n est ou n'est pas premier à $2D_1$. Quant aux deux conditions que ce lemme suppose, et qui consistent 1^o. en ce que c_n doit être une fonction périodique de l'indice n , et 2^o. en ce que la somme des termes qui composent une période, doit être zéro, on s'assure facilement qu'elles sont remplies. Cela est évident pour la première, et pour voir que la seconde a également lieu, il suffira de recourir au lemme qui termine le §. 5, et de remarquer qu'on ne saurait avoir à la fois $\delta = 1$, $\varepsilon = 1$, $P = \pm 1$. En effet, il résulte des conditions (9) que les équations précédentes ne sont compatibles entre elles que lorsqu'on a $P = 1$: ces équations se rapportent alors au cas que nous avons exclu où le déterminant est un carré positif. Il résulte de ce qui précède que la somme:

$$\sum \delta^{\frac{1}{2}(n-1)} \varepsilon^{\frac{1}{2}(n^2-1)} \binom{n}{P} \frac{1}{n^{1+e}},$$

lorsqu'on y considère la variable positive comme devenant infiniment petite, converge vers une limite finie donnée par l'expression:

$$(14) \quad \sum \delta^{\frac{1}{2}(n-1)} \varepsilon^{\frac{1}{2}(n^2-1)} \binom{n}{P} \frac{1}{n},$$

dans laquelle il faut supposer que les valeurs de n se suivent dans l'ordre naturel, c'est-à-dire de manière à former une suite croissante.

1. Revenons maintenant à l'équation (12), et considérons en premier lieu le cas où D est négatif de sorte que $D = -D_1$. Soient

$$(15) \quad ax^2 + 2bxy + cy^2, \quad a'x^2 + 2b'xy + c'y^2, \quad \dots$$

les formes différentes et proprement primitives de ce déterminant D , formes dont je désignerai le nombre par h . Cela étant, on aura l'égalité:

$$(16) \quad \sum \frac{2^{u+1}}{m^2} = \sum \frac{1}{(ax^2 + 2bxy + cy^2)^s} + \sum \frac{1}{(a'x^2 + 2b'xy + c'y^2)^s} + \dots,$$

où le second membre contient autant de termes qu'il y a de formes (15), et où la double sommation dans chaque terme doit s'étendre à tous les systèmes de valeurs entières de x et de y , comprises entre $-\infty$ et ∞ , qui remplissent

la double condition de n'avoir pas de diviseur commun et de donner à la forme où elles sont substituées, une valeur première à $2D$. Cela résulte 1°. de ce que chacun des entiers m contenus dans le premier membre est, en vertu du théorème I du §. 4, susceptible d'être représenté de la manière indiquée et par l'ensemble des formes (15), autant de fois qu'il y a d'unités dans l'expression 2^{a+1} , et 2°. de ce que réciproquement toute valeur première à $2D$, que l'une quelconque des formes (15) peut obtenir lorsqu'on y attribue à x et y des valeurs sans diviseur commun, coïncide d'après les résultats connus et que nous avons rappelés au commencement du paragraphe cité, avec l'un des entiers désignés par m . Si maintenant l'on substitue l'expression de $\Sigma \frac{2^{a+1}}{m^s}$, donnée par l'équation précédente, dans l'équation (12), il viendra :

$$\begin{aligned} \Sigma \frac{1}{n^{2s}} \cdot \Sigma \frac{1}{(ax^2+2bxy+cy^2)^s} + \Sigma \frac{1}{n^{2s}} \cdot \Sigma \frac{1}{(a'x^2+2b'xy+c'y^2)^s} + \dots \\ = 2 \Sigma \frac{1}{n^s} \cdot \Sigma \delta^{s(n-1)} \epsilon^{\frac{1}{2}(n^2-1)} \binom{n}{P} \frac{1}{n^s}. \end{aligned}$$

Il est facile de voir que chacun des termes du premier membre peut être mis sous une forme plus simple. Le premier de ces termes est évidemment équivalent à l'expression :

$$\Sigma' \frac{1}{(ax^2+2bxy+cy^2)^s},$$

où les valeurs simultanées de x et de y , dans la sommation double, ne sont plus assujetties qu'à la condition unique de rendre le trinôme où elles sont substituées, impair et premier à D . En attachant donc ce sens au signe Σ' , on aura :

$$(17) \quad \left\{ \begin{aligned} \Sigma' \frac{1}{(ax^2+2bxy+cy^2)^s} + \Sigma' \frac{1}{(a'x^2+2b'xy+c'y^2)^s} + \dots \\ = 2 \Sigma \frac{1}{n^s} \cdot \Sigma \delta^{s(n-1)} \epsilon^{\frac{1}{2}(n^2-1)} \binom{n}{P} \frac{1}{n^s}. \end{aligned} \right.$$

Il faut maintenant poser $s = 1 + q$, la variable positive q étant toujours considérée comme infiniment petite, et voir ce que les différents termes du premier membre deviendront dans cette supposition. Puisque d'après les résultats que nous avons établis dans le §. 5, les valeurs simultanées que l'on doit attribuer à x et y , dans chacune de ces sommes doubles, dans la première par exemple, peuvent être distribuées en systèmes de la forme :

$$(18) \quad x = 2D_1 v + a, \quad y = 2D_1 w + \gamma,$$

on voit que la somme en question peut être décomposée en autant de sommes partielles qu'il y a de ces systèmes, telles que:

$$\Sigma \frac{1}{(ax^2+2bxy+cy^2)^{1+\nu}},$$

où il faut substituer pour x et y les expressions précédentes, et sommer ensuite relativement aux entiers v et w , depuis $-\infty$ jusqu'à ∞ . Pour obtenir cette somme partielle, nous chercherons l'entier qui exprime combien de fois le trinôme $ax^2+2bxy+cy^2$, dans cette somme, obtient une valeur ne surpassant pas la quantité positive quelconque σ . Or, cette dernière question est évidemment identique à celle de savoir combien dans l'intérieur ou sur le contour de l'ellipse, déterminée par l'équation:

$$ax^2+2bxy+cy^2 = \sigma,$$

il y a de points dont les coordonnées x et y sont de la forme (18), et si l'on observe que l'aire de cette ellipse est:

$$\frac{\pi}{\sqrt{(ac-b^2)}} \sigma = \frac{\pi}{\sqrt{D_1}} \sigma,$$

où la lettre π a la signification ordinaire, on conclura immédiatement du second lemme du §. 1*) que le nombre qu'il s'agit de déterminer, peut être mis sous la forme:

$$\frac{\pi}{4\sqrt{D_1}} \sigma + \sigma^\delta \psi(\sigma)$$

l'exposant constant δ ayant une valeur quelconque comprise entre $\frac{1}{2}$ et 1, et la fonction $\psi(\sigma)$ restant finie quelque grande que l'on suppose la variable σ . Il résulte de là et du premier théorème du paragraphe déjà cité, que la somme partielle que nous considérons, a la valeur:

$$\frac{\pi}{4\sqrt{D_1}} \cdot \frac{1}{\varrho},$$

d'où l'on conclut, en considérant que d'après le §. 5, le nombre des systèmes (18) et par suite celui des sommes partielles dans lesquelles la somme:

$$\Sigma' \frac{1}{(ax^2+2bxy+cy^2)^{1+\nu}}$$

*) Il est évident par la nature de ce lemme, que les points placés sur le contour de la courbe peuvent être considérés à volonté comme des points intérieurs ou comme des points extérieurs. On peut donc aussi et à plus forte raison, ranger ces points en partie parmi les points intérieurs et en partie parmi les points extérieurs, comme nous le ferons plus bas, lorsque nous nous occuperons des déterminants positifs.

a été partagée, est $2D_1A$ ou $4D_1A$, selon que D est impair ou pair, que la somme précédente est suivant ces deux cas :

$$\frac{\pi A}{2\sqrt{D_1^3}} \cdot \frac{1}{\varrho} \quad \text{ou} \quad \frac{\pi A}{\sqrt{D_1^3}} \cdot \frac{1}{\varrho}.$$

Comme ce résultat ne contient rien qui soit particulier à la forme $ax^2 + 2bxy + cy^2$, et qu'il ne renferme que le déterminant commun à toutes les formes (15), on voit que le premier membre de l'équation (17), en supposant toujours ϱ infiniment petit et en distinguant le cas de D impair et celui de D pair, est :

$$\frac{h\pi A}{2\sqrt{D_1^3}} \cdot \frac{1}{\varrho} \quad \text{ou} \quad \frac{h\pi A}{\sqrt{D_1^3}} \cdot \frac{1}{\varrho}.$$

Au moyen de ces expressions et des résultats (13) et (14), précédemment établis, l'équation (17) se changera pour une valeur infiniment petite de ϱ , dans l'équation remarquable qui suit et où les cas de D pair et impair sont confondus dans la même forme :

$$(19) \quad h = \frac{2}{\pi} \sqrt{D} \Sigma \delta^{A(n-1)} \varepsilon^{\frac{1}{3}(n^2-1)} \left(\frac{n}{P} \right) \frac{1}{n}.$$

Cette équation est sujette à une exception qui a lieu lorsque D est -1 , et qui est une suite de l'exception que le théorème I du §. 4 souffre dans le même cas. Pour rétablir l'exactitude dans ce cas singulier, il faut doubler le second membre, comme cela résulte de l'analyse précédente, et comme on peut aussi le vérifier *à posteriori*. En effet, on a dans ce cas $h = 1$, $D_1 = 1$, $\delta = -1$, $\varepsilon = 1$, $P = -1$; l'équation modifiée, comme on vient de le dire, deviendra donc :

$$1 = \frac{4}{\pi} \left(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots \right),$$

ce qui est exact d'après la série connue de LEIBNIZ.

II. Le déterminant D étant toujours négatif et en outre tel que $D \equiv 1 \pmod{4}$, nous supposerons que les formes (15) sont celles de l'ordre improprie primitif. On aura dans cette supposition, $\delta = 1$, $\varepsilon = 1$, et l'égalité (16) devra être remplacée par celle-ci :

$$\Sigma \frac{2^{\mu+1}}{(2m)^{\mu}} = \Sigma \frac{1}{(ax^2 + 2bxy + cy^2)^{\mu}} + \Sigma \frac{1}{(a'x^2 + 2b'xy + c'y^2)^{\mu}} + \dots,$$

où la double sommation s'étend dans chaque terme à toutes les valeurs simultanées de x et de y qui n'ont pas de diviseur commun, et qui vendent la moitié de la forme entrant dans ce terme, première à $2D$. La substitution de l'ex-

pression précédente dans l'équation (12) donne:

$$\begin{aligned} \Sigma \frac{1}{n^{2s}} \cdot \Sigma \frac{1}{(ax^2 + 2bxy + cy^2)^s} + \Sigma \frac{1}{n^{2s}} \cdot \Sigma \frac{1}{(a'x^2 + 2b'xy + c'y^2)^s} + \dots \\ = 2^{1-s} \Sigma \frac{1}{n^s} \cdot \Sigma \left(\frac{n}{P} \right) \frac{1}{n^s}, \end{aligned}$$

équation de laquelle on passe, comme dans le cas déjà examiné, à cette autre:

$$(20) \quad \left\{ \begin{aligned} \Sigma' \frac{1}{(ax^2 + 2bxy + cy^2)^s} + \Sigma' \frac{1}{(a'x^2 + 2b'xy + c'y^2)^s} + \dots \\ = 2^{1-s} \Sigma \frac{1}{n^s} \cdot \Sigma \left(\frac{n}{P} \right) \frac{1}{n^s}, \end{aligned} \right.$$

le signe Σ' indiquant que dans la double sommation la moitié de la forme quadratique ne doit recevoir que des valeurs premières à $2D$. En supposant maintenant $s = 1 + \rho$, ρ étant toujours une variable infiniment petite et positive, on achèvera la solution comme dans le cas déjà traité, si l'on se rappelle que d'après ce qui a été démontré dans le §. 5, le nombre des systèmes de la forme:

$$x = 2D_1 v + a, \quad y = 2D_1 w + \gamma,$$

qui rendent la moitié d'une forme improprement primitive du déterminant D première à $2D$, est $D_1 \mathcal{A}$ ou $3D_1 \mathcal{A}$, suivant que l'on a $D \equiv 1$ ou $D \equiv 5 \pmod{8}$. On trouve ainsi pour le nombre h des formes improprement primitives:

$$(21) \quad \left\{ \begin{aligned} h &= \frac{2}{\pi} \sqrt{D_1} \Sigma \left(\frac{n}{P} \right) \frac{1}{n}, & D &\equiv 1 \pmod{8}, \\ h &= \frac{1}{3} \frac{2}{\pi} \sqrt{D_1} \Sigma \left(\frac{n}{P} \right) \frac{1}{n}, & D &\equiv 5 \pmod{8}. \end{aligned} \right.$$

On doit ajouter que la seconde de ces équations est en défaut lorsqu'on a $D = -3$, comme cela résulte de l'exception à laquelle le théorème I du §. 4 est sujet dans le même cas, et que pour rétablir l'exactitude, le second membre doit être triplé.

III. Nous passons maintenant au cas des déterminants positifs, c'est-à-dire au cas où l'on a $D = D_1$, et nous supposons d'abord que les formes différentes (15) appartiennent à l'ordre proprement primitif, et remplissent chacune les conditions (7) du §. 4. On a alors d'après le théorème III du §. 4:

$$\Sigma \frac{2^u}{m^s} = \Sigma \frac{1}{(ax^2 + 2bxy + cy^2)^s} + \Sigma \frac{1}{(a'x^2 + 2b'xy + c'y^2)^s} + \dots$$

où la double sommation dans chacun des termes du second membre doit s'étendre

à tous les systèmes de valeurs simultanées de x et y , premières entre elles, qui donnent au trinôme où elles sont substituées, une valeur première à $2D$ et satisfont en outre aux inégalités (8) du paragraphe cité, lorsqu'il s'agit du premier terme, et à des inégalités de forme analogue pour tous les autres termes.

Comme les nombres susceptibles d'être exprimés par une forme de déterminant positif, peuvent être positifs ou négatifs, il semble d'abord que l'on doive ajouter encore la condition que les indéterminées soient choisies de manière à donner à la forme quadratique une valeur positive; mais il est aisé de voir que cette condition est déjà implicitement contenue dans les précédentes. En effet, a , b , x et y étant positifs, la condition:

$$x \geq \frac{T-bU}{aU'}y$$

entraînera évidemment celle-ci:

$$ax^2+2bxy+cy^2 \geq \frac{y^2}{aU'^2} (T^2-(b^2-ac)U^2) = \frac{y^2}{aU'^2}.$$

L'expression précédente de $\sum \frac{2^\mu}{m^s}$ étant substituée dans l'équation (12), il viendra:

$$\begin{aligned} \sum \frac{1}{n^{2s}} \cdot \sum \frac{1}{(ax^2+2bxy+cy^2)^s} + \sum \frac{1}{n^{2s}} \cdot \sum \frac{1}{(a'x^2+2b'xy+c'y^2)^s} + \dots \\ = \sum \frac{1}{n^s} \cdot \sum \delta^{\frac{1}{2}(n-1)} \varepsilon^{\frac{1}{2}(n^2-1)} \left(\frac{n}{P}\right) \frac{1}{n^s}. \end{aligned}$$

On voit sans peine que le produit:

$$\sum \frac{1}{n^s} \cdot \sum \frac{1}{(ax^2+2bxy+cy^2)^s}$$

peut être mis sous cette forme plus simple:

$$\sum' \frac{1}{(ax^2+2bxy+cy^2)^s},$$

où la double sommation est supposée s'étendre à toutes les valeurs simultanées de x et y , qui rendent le trinôme premier à $2D$, et en outre telles que l'on ait:

$$x > 0, \quad y > 0, \quad y \leq \frac{aU}{T-bU'}x.$$

Il suffit pour cela de remarquer que les conditions (8) du §. 4 conservent la même forme lorsqu'on y remplace x et y par nx et ny , n étant positif, et que si l'on écrit ensuite x et y au lieu de nx et ny , les nouvelles indéterminées x et y ne seront plus assujetties à la condition d'être premières entre elles. En

attachant donc au signe Σ' le sens que l'on vient de définir et en supposant, bien entendu, que s'il s'agit de la seconde forme, a, b dans la dernière des inégalités précédentes doivent être remplacées par a', b' , et ainsi de suite, on aura l'équation:

$$(22) \quad \left\{ \begin{aligned} & \Sigma' \frac{1}{(ax^2 + 2bxy + cy^2)^s} + \Sigma' \frac{1}{(a'x^2 + 2b'xy + c'y^2)^s} + \dots \\ & = \Sigma \frac{1}{n^s} \cdot \Sigma j^{\frac{1}{2}(n-1)} \varepsilon^{\frac{1}{2}(n-1)} \left(\frac{n}{P} \right) \frac{1}{n^s}. \end{aligned} \right.$$

Il s'agira maintenant de voir ce que les différents termes de cette équation deviendront, lorsqu'après avoir posé $s = 1 + \varrho$, la variable positive ϱ devient moindre que toute grandeur donnée. A cet effet, nous décomposerons chacun des termes du premier membre, le premier:

$$\Sigma' \frac{1}{(ax^2 + 2bxy + cy^2)^{1+\varrho}},$$

par exemple, en autant de sommes partielles qu'il y a de systèmes de la forme:

$$x = 2Dr + a, \quad y = 2Dw + \gamma,$$

qui rendent le trinôme $ax^2 + 2bxy + cy^2$ premier à $2D$. Soit:

$$\Sigma \frac{1}{(ax^2 + 2bxy + cy^2)^{1+\varrho}}; \quad x > 0, \quad y > 0, \quad y \leq \frac{aU}{T-bU} x, \\ x = 2Dv + a, \quad y = 2Dw + \gamma.$$

l'une de ces sommes partielles, dans laquelle la sommation double relative à v et w doit s'étendre à toutes les valeurs entières depuis $-\infty$ jusqu'à $+\infty$). Pour obtenir l'expression de cette somme, nous désignerons par σ une variable positive quelconque, et nous chercherons le nombre qui exprime combien de fois le trinôme $ax^2 + 2bxy + cy^2$ dans la double sommation obtient une valeur non-supérieure à σ . Or, d'après la construction géométrique indiquée dans le §. 4, la recherche dont il s'agit, revient évidemment à la question de savoir combien dans l'intérieur ou sur le contour du secteur hyperbolique, terminé d'une part par les droites:

$$y = 0, \quad y = \frac{aU}{T-bU} x,$$

et de l'autre par l'arc de la première branche de l'hyperbole:

$$ax^2 + 2bxy + cy^2 = \sigma,$$

*) Compatibles avec les conditions précédentes.¹⁾

¹⁾ Anmerkung von Dirichlet's Hand in dem an Gauss gesandten Exemplar. K.

il y a de points dont les coordonnées x et y sont de la forme:

$$x = 2Dv + a, \quad y = 2Dw + \gamma.$$

Ajoutons, pour être tout à fait exact, quoique cela n'influe en rien sur le résultat définitif, que l'on doit faire abstraction de ceux des points en question qui pourraient se trouver sur la partie du contour, formée par l'axe de x . Si l'on a recours aux coordonnées polaires r et φ , liées aux coordonnées rectangulaires x et y par les équations $x = r \cos \varphi$, $y = r \sin \varphi$, l'aire du secteur sera:

$$\frac{1}{2} \int r^2 d\varphi = \frac{1}{2} \sigma \int \frac{d\varphi}{a \cos^2 \varphi + 2b \cos \varphi \sin \varphi + c \sin^2 \varphi},$$

les limites de l'intégrale étant zéro et l'angle aigu dont la tangente trigonométrique est $\frac{aU}{T-bU}$. L'intégration étant effectuée par les méthodes connues, on trouvera pour l'aire dont il s'agit, cette expression très simple:

$$\frac{\sigma}{2\sqrt{D}} \log(T+U\sqrt{D}).$$

Au moyen de ce résultat et du second lemme du §. 1, on conclura que le nombre que nous nous étions proposé de déterminer, peut être mis sous la forme:

$$\frac{\sigma}{8\sqrt{D^3}} \log(T+U\sqrt{D}) + \sigma^\delta \psi(\sigma).$$

L'exposant constant δ étant compris entre $\frac{1}{2}$ et 1, et la fonction $\psi(\sigma)$ restant finie, quelque grande que l'on suppose la variable σ . Il suit de là et du premier des théorèmes du §. 1, que la somme partielle que nous considérons, est:

$$\frac{1}{8\sqrt{D^3}} \log(T+U\sqrt{D}) \frac{1}{\varrho},$$

et comme d'après les résultats du §. 5, le nombre des sommes partielles contenues dans la même somme totale, est $4D\mathcal{A}$ ou $2D\mathcal{A}$, suivant que D est pair ou impair, on conclura que chacun des termes du premier membre de l'équation (22) est selon ces deux cas, et pour une valeur infiniment petite de ϱ :

$$\frac{\mathcal{A}}{2\sqrt{D^3}} \log(T+U\sqrt{D}) \frac{1}{\varrho}, \quad \text{ou} \quad \frac{\mathcal{A}}{4\sqrt{D^3}} \log(T+U\sqrt{D}) \frac{1}{\varrho}.$$

Si donc nous désignons par h le nombre des formes différentes du déterminant D , le premier membre sera:

$$\frac{h\mathcal{A}}{2\sqrt{D^3}} \log(T+U\sqrt{D}) \frac{1}{\varrho}, \quad \text{ou} \quad \frac{h\mathcal{A}}{4\sqrt{D^3}} \log(T+U\sqrt{D}) \frac{1}{\varrho},$$

selon que D est pair ou impair.

Comme, d'un autre côté et en vertu des résultats (13) et (14), le second membre est respectivement dans ces deux cas :

$$\frac{J}{D} \cdot \frac{1}{q} \Sigma \delta^{\frac{1}{2}(n-1)} \epsilon^{\frac{1}{2}(n^2-1)} \left(\frac{n}{P}\right) \frac{1}{n} \quad \text{ou} \quad \frac{J}{2D} \cdot \frac{1}{q} \Sigma \delta^{\frac{1}{2}(n-1)} \epsilon^{\frac{1}{2}n^2-1} \left(\frac{n}{P}\right) \frac{1}{n}.$$

on conclura, en supprimant le facteur $\frac{1}{q}$, commun aux deux membres :

$$(23) \quad h = \frac{2\sqrt{D}}{\log(T+U\sqrt{D})} \Sigma \delta^{\frac{1}{2}(n-1)} \epsilon^{\frac{1}{2}(n^2-1)} \left(\frac{n}{P}\right) \frac{1}{n},$$

équation qui convient à un déterminant positif (non-carré) quelconque, pair ou impair, et dans laquelle T et U sont les plus petits entiers positifs, autres que 1 et 0, qui satisfont à l'équation $t^2 - Du^2 = 1$.

IV. Le cas où le déterminant positif D est de la forme $4\nu+1$, et où les formes de ce déterminant dont il s'agit de déterminer le nombre h , sont celles de l'ordre improprement primitif, étant entièrement semblable à celui que nous venons de traiter en détail, nous nous contenterons de rapporter le résultat qui répond à ce cas, et qui est contenu dans les équations qui suivent :

$$(24) \quad \begin{cases} h = \frac{2\sqrt{D}}{\log_{\frac{1}{2}}(T+U\sqrt{D})} \Sigma \left(\frac{n}{P}\right) \frac{1}{n}, & D \equiv 1 \pmod{8}, \\ h = \frac{1}{3} \frac{2\sqrt{D}}{\log_{\frac{1}{2}}(T+U\sqrt{D})} \Sigma \left(\frac{n}{P}\right) \frac{1}{n}. & D \equiv 5 \pmod{8}. \end{cases}$$

dans lesquelles T et U désignent les moindres entiers positifs, autres que 2 et 0, qui satisfont à l'équation $t^2 - Du^2 = 4$.

V. Nous nous occuperons maintenant de la recherche déjà indiquée dans le §. 3, en prouvant que les genres énumérés d'après les principes connus et que nous avons rappelés dans le paragraphe cité, existent tous réellement et contiennent chacun le même nombre de formes. Soient à cet effet :

$$(25) \quad g. \quad g'. \quad g''. \quad \dots \quad || \quad \psi. \quad \psi'. \quad \psi''. \quad \dots$$

les expressions qui servent à faire cette énumération pour un déterminant quelconque, soit qu'il s'agisse des formes proprement primitives, soit qu'il s'agisse de celles qui composent l'ordre improprement primitif, lorsque ce dernier ordre existe pour le déterminant donné. Les déterminants carrés étant exclus, la première partie de la ligne précédente contiendra au moins un terme, et il résulte de l'inspection des deux tableaux donnés dans le §. 3, que les expressions

g, g', g'', \dots qui forment cette première partie, sont toujours telles qu'on ait:

$$(26) \quad g g' g'' \dots = \delta^{\frac{1}{2}(m-1)} \epsilon^{\frac{1}{2}(m^2-1)} \left(\frac{m}{P}\right).$$

Nous désignerons généralement par χ l'une quelconque des expressions (25), ou l'un quelconque des produits que l'on peut former avec ces expressions, en les combinant 2 à 2, 3 à 3, et ainsi de suite, ou enfin le produit de toutes, en n'excluant que le seul produit (26), autrement dit, nous désignerons par χ l'un quelconque des termes de l'expression développée:

$$(27) \quad [(1+g)(1+g')(1+g'')\dots][(1+\psi)(1+\psi')(1+\psi'')\dots] - g g' g'' \dots - 1.$$

Si nous conservons à la lettre χ la même signification que nous lui avons donnée dans le §. 3, le nombre des expressions χ sera $2^k - 2$. Cela supposé, nous allons faire voir que si l'on partage le nombre total h des formes qui répondent au déterminant donné, en deux groupes comprenant respectivement H et H' formes, en rangeant dans le premier groupe toutes celles qui satisfont à la condition $\chi = 1$, et dans le second celles qui remplissent la condition opposée $\chi = -1$, on aura toujours:

$$H - H' = 0.$$

Pour prouver ce dont il s'agit, il suffira d'appliquer l'analyse dont nous avons fait usage, en partant de l'équation (12), à l'équation plus générale (11), après avoir attribué dans cette dernière à θ, η, P_2 et R_1 des valeurs qui font coïncider l'expression $\theta^{\frac{1}{2}(m-1)} \eta^{\frac{1}{2}(m^2-1)} \left(\frac{m}{P_2 R_1}\right)$ avec χ . Il est facile de voir qu'en remplissant cette condition, il ne peut arriver qu'on ait à la fois, soit:

$$\theta = 1, \quad \eta = 1, \quad P_2 R_1 = \pm 1,$$

soit:

$$\delta\theta = 1, \quad \epsilon\eta = 1, \quad P_1 R_1 = \pm 1.$$

L'impossibilité du premier système de valeurs simultanées résulte de ce que χ contient au moins un facteur de l'une des formes:

$$(-1)^{\frac{1}{2}(m-1)}, \quad (-1)^{\frac{1}{2}(m^2-1)}, \quad \left(\frac{m}{P}\right), \quad \left(\frac{m}{r}\right);$$

et pour que le second pût avoir lieu, il faudrait que l'on eût $\theta = \delta, \eta = \epsilon, P_2 R_1 = \pm P$, ce qui donnerait à χ la forme:

$$\delta^{\frac{1}{2}(m-1)} \epsilon^{\frac{1}{2}(m^2-1)} \left(\frac{m}{P}\right) = g g' g'' \dots,$$

que nous avons exclue plus haut. Il résulte de là que chacun des deux facteurs du second membre de l'équation (11) est de même nature que le second facteur du second membre de l'équation (12), et que par conséquent ces deux facteurs convergent l'un et l'autre vers une limite finie de la forme (14), lorsque la variable ϱ devient infiniment petite. Pour discuter le premier membre de l'équation (11) dans la même circonstance, il faudra substituer à l'égalité (16), lorsqu'il s'agit d'un déterminant négatif et de l'ordre proprement primitif, celle-ci :

$$\Sigma \chi \frac{2^{u+1}}{m^2} = \pm \Sigma \frac{1}{(ax^2 + 2bxy + cy^2)^2} \pm \Sigma \frac{1}{(ax^2 + 2b'xy + c'y^2)^2} \pm \dots,$$

où l'on doit choisir le signe supérieur ou le signe inférieur dans chacun des termes du second membre, suivant que la forme que ce terme contient, satisfait à la condition $\chi = 1$, ou à $\chi = -1$, et il faudra faire une substitution analogue dans les trois autres cas. Cela posé, on voit sans peine et sans qu'il soit nécessaire d'entrer dans aucun détail à cet égard, que le premier membre de l'équation (11), en y supposant toujours la variable ϱ infiniment petite, sera, abstraction faite d'un facteur purement numérique, et qui varie suivant les quatre cas, le produit de $(H - H') \frac{1}{\varrho}$ et d'une expression telle que :

$$\frac{A}{\sqrt{D_1^3}} \pi, \quad \frac{A}{\sqrt{D^3}} \log(T + U \sqrt{D}) \quad \text{ou} \quad \frac{A}{\sqrt{D^3}} \log \frac{1}{2}(T + U \sqrt{D}).$$

Or, cette dernière expression étant manifestement différente de zéro, il faut, pour que le premier membre reste fini comme le second, qu'on ait :

$$H - H' = 0,$$

ce qu'il s'agissait de faire voir.

Au moyen de ce résultat, il nous sera facile de prouver que les formes sont également réparties entre les genres énumérés d'après les règles du §. 3. Soit pour abrégier $2^{\lambda-1} = z$, et désignons par $h_1, h_2, h_3, \dots, h_x$ les nombres des formes contenues dans les différents genres, rangés dans un ordre quelconque, les termes de la suite précédente qui répondraient à des genres non-existants étant supposés égaux à zéro. Si maintenant l'on remarque que les formes qui composent un même genre, satisfont tous ou à la condition $\chi = 1$, ou à la condition opposée $\chi = -1$, il est évident que toute équation de la forme :

$$H - H' = 0$$

peut s'écrire comme il suit :

$$(28) \quad h_1 \pm h_2 \pm h_3 \pm \dots \pm h_x = 0.$$

Nous avons donné dans cette équation le signe + au premier terme; le signe de tout autre terme est + ou -, selon que le genre auquel ce terme correspond, satisfait à la même condition $\chi = \pm 1$ que celui auquel se rapporte h_1 , ou à la condition opposée. Il s'agira maintenant d'examiner combien de fois, dans l'ensemble des équations analogues à la précédente et dont le nombre est $2^{\lambda}-2$, comme celui des expressions χ , un terme quelconque h_w , autre que le premier, a le signe + ou le signe -, ou autrement dit, combien de fois ce terme a un signe égal ou opposé à celui du premier terme. Soit à cet effet:

$$g = a, \quad g' = a', \quad g'' = a'', \quad \dots \quad | \quad \psi = \beta, \quad \psi' = \beta', \quad \psi'' = \beta'', \quad \dots$$

le caractère complet du genre pour lequel h_1 désigne le nombre des formes, $a, a', a'', \dots; \beta, \beta', \beta'', \dots$ étant des valeurs déterminées de la forme ± 1 , dont les premières satisfont à la condition $aa'a''\dots = 1$. Soit de même:

$$g = a, \quad g' = a', \quad g'' = a'', \quad \dots \quad | \quad \psi = b, \quad \psi' = b', \quad \psi'' = b'', \quad \dots$$

le caractère complet du genre auquel se rapporte h_w . Cela posé, il suffit de se reporter à l'expression (27) dont le développement donne toutes les expressions χ , pour voir que l'excès du nombre des cas où h_1 et h_w ont le même signe, sur celui où ils sont précédés de signes opposés, sera donné par l'expression qui suit:

$$[(1+aa)(1+a'a')\dots][(1+\beta b)(1+\beta'b')\dots] - aa'a''\dots - 1.$$

Or les deux caractères complets étant différents, on ne saurait avoir à la fois:

$$aa = 1, \quad a'a' = 1, \quad \dots; \quad \beta b = 1, \quad \beta'b' = 1, \quad \dots;$$

la première partie de l'expression précédente a donc la valeur zéro, et comme l'on a évidemment:

$$aa.a'a''\dots = 1,$$

l'excès dont il s'agit a la valeur -2. Il suit de là que si l'on ajoute toutes les équations de la forme (28), dont le nombre est $2^{\lambda}-2$, et l'équation évidente:

$$2h_1 + 2h_2 + 2h_3 + \dots + 2h_x = 2h,$$

il en résultera celle-ci: $2^{\lambda}h_1 = 2h$, et par suite $h_1 = \frac{h}{2^{\lambda-1}}$, ce qui prouve que la totalité des formes se partage également entre les différents genres, le genre auquel se rapporte le nombre h_1 , ayant été arbitrairement choisi.

On a ainsi une démonstration nouvelle et très simple de l'un des principaux théorèmes de la théorie des formes quadratiques et qui n'avait été établi

jusqu'à présent que par le concours d'un grand nombre de considérations diverses. Voyez l'ouvrage de M. GAUSS, art. 252, 261 et 287, III.

Il nous resterait maintenant à développer les théorèmes que contiennent les équations établies dans les quatre numéros précédents de ce paragraphe et qui sont de deux espèces, les uns résultant des expressions de h telles que nous les avons obtenues dans ce qui précède, les autres exigeant au contraire que l'on effectue préalablement les sommations indiquées dans ces expressions, pour que le nombre h se présente sous une forme purement arithmétique. Comme les résultats dont il s'agit, sont très nombreux et pour la plupart entièrement nouveaux, il sera convenable de les présenter avec quelque étendue. Par cette raison j'en remettrai l'exposition à la continuation de ces recherches, et je terminerai cette première partie, en remplissant l'engagement que j'ai pris dans le mémoire déjà cité sur la progression arithmétique. D'après le §. 11 de ce mémoire*), il reste à prouver que la somme:

$$\Sigma(\pm 1)^{\alpha}(\pm 1)^{\beta}(\pm 1)^{\gamma}(\pm 1)^{\delta} \dots \frac{1}{n}$$

dans laquelle les signes supérieurs n'ont pas simultanément lieu, a une valeur différente de zéro.

Partageons les nombres premiers positifs p, p', p'', \dots auxquels se rapportent les valeurs ambiguës de la forme ± 1 , à partir de la troisième, en deux groupes, en comprenant dans le premier groupe tous ceux de ces nombres premiers, auxquels le signe inférieur correspond. En continuant à représenter par p, p', p'', \dots les nombres du premier groupe, soit:

$$\pm p p' p'' \dots = P,$$

le double signe restant à fixer; soient encore r, r', r'', \dots ceux du second groupe et posons:

$$r r' r'' \dots = R.$$

Cela posé, il résulte de la signification des lettres $\alpha, \beta, \gamma, \delta, \dots$ expliquée dans le §. 7 du mémoire cité, que la somme précédente peut être mise sous la forme:

$$\Sigma(\pm 1)^{k(n-1)}(\pm 1)^{l, n^2-1} \left(\frac{n}{P}\right) \frac{1}{n}.$$

Si maintenant l'on suppose le signe arbitraire dans l'équation:

$$\pm p p' p'' \dots = P.$$

*) S. 341 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

tellement choisi que le nombre P soit de la forme $4\mu + 1$ ou de la forme $4\mu + 3$, suivant que le signe donné dans l'expression $(\pm 1)^{\frac{1}{2}(n-1)}$ est le signe supérieur ou inférieur, il est évident que la somme précédente coïncidera avec celle que contient l'expression obtenue plus haut pour le nombre h des formes qui répondent au déterminant D , en supposant ce déterminant égal à PR^2 ou à $2PR^2$, suivant que le signe donné dans l'expression $(\pm 1)^{\frac{1}{2}(n'-1)}$ est le signe supérieur ou le signe inférieur. On conclut de là que la somme que nous avons à considérer, est en effet toujours différente de zéro, puisque, s'il en était autrement, le nombre h se réduirait lui-même à zéro, ce qui est impossible, comme on le voit par la forme $x^2 - Dy^2$, qui a lieu quel que soit le déterminant D .*)

§. 7.

Nous allons maintenant développer les conséquences qui dérivent des équations établies dans les 4 premiers numéros du paragraphe précédent, en commençant par celles qui s'obtiennent indépendamment de la sommation des deux séries générales contenues dans les expressions de h . Nous passerons ensuite à celles qui résultent de cette sommation, que l'on peut effectuer soit par l'intégration d'une fraction rationnelle, soit au moyen des séries connues de sinus ou de cosinus.

Reprenons l'équation (17), dans laquelle les deux sommations relatives à n doivent s'étendre à tous les entiers positifs impairs et premiers au déterminant négatif D . Si dans la première de ces deux sommes l'on écrit n' à la place de n , l'équation pourra se mettre sous la forme:

$$(1) \quad \Sigma' \frac{1}{(a^2x^2 + 2bxy + cy^2)^s} + \Sigma' \frac{1}{(a'^2x^2 + 2b'xy + c'y^2)^s} + \dots = 2 \Sigma \delta^{\frac{1}{2}(n-1)} \epsilon^{\frac{1}{2}(n'-1)} \left(\frac{n}{P}\right) \frac{1}{(nn')^s},$$

le signe Σ indiquant une double sommation relative à n et n' . Il est facile de donner à cette série la forme d'une série simple, en réunissant en un seul tous les termes pour lesquels le produit nn' a la même valeur. On aura ainsi pour terme général $\sigma_n \frac{1}{n^s}$, n ayant toujours la même signification que précédemment, et σ_n désignant l'excès du nombre des diviseurs k de n qui satisfont à la condition:

$$\delta^{\frac{1}{2}(k-1)} \epsilon^{\frac{1}{2}(k^2-1)} \left(\frac{k}{P}\right) = 1,$$

*) Hier schliesst der erste im 19. Bande des CRELLE'schen Journals abgedruckte, vom 4 Juli 1839 datirte Theil der Abhandlung. K.

sur celui de ces diviseurs qui satisfont à la condition opposée:

$$\delta^{1/2(k-1)} \varepsilon^{1/2(l^2-1)} \left(\frac{k}{P} \right) = -1.$$

Le premier membre peut également se réduire à une série simple de forme analogue et dont le terme général a pour coefficient le nombre qui exprime combien de fois l'entier n peut être représenté par la totalité des formes quadratiques, en attribuant aux indéterminées x et y de ces formes des valeurs quelconques positives ou négatives, premières entre elles ou non. En désignant le nombre dont il s'agit par τ_n , on aura:

$$\Sigma \tau_n \frac{1}{n^s} = 2 \Sigma \sigma_n \frac{1}{n^s}.$$

Cette équation ayant lieu pour toute valeur de l'indéterminée s , supérieure à l'unité, il est facile d'en conclure qu'on a $\tau_n = 2\sigma_n$.

Ce résultat et celui qui se déduit de la même manière de l'équation (20), après en avoir mis le second membre sous la forme:

$$2 \Sigma \left(\frac{n}{P} \right) \frac{1}{(2nn')^s},$$

peuvent être réunis dans l'énoncé commun que voici et dans lequel nous distinguons en formes de première et de seconde espèce celles que nous avons appelées précédemment proprement et improprement primitives*).

n étant un entier positif impair et premier au déterminant négatif D , si l'on désigne par σ l'excès du nombre des diviseurs k de n qui sont tels qu'on ait $\delta^{1/2(k-1)} \varepsilon^{1/2(l^2-1)} \left(\frac{k}{P} \right) = 1$ (où δ , ε et P ont la signification que nous avons fixée au §. 6), sur celui de ces diviseurs qui remplissent la condition opposée $\delta^{1/2(k-1)} \varepsilon^{1/2(l^2-1)} \left(\frac{k}{P} \right) = -1$, le double du nombre σ exprimera de combien de manières différentes l'entier n ($2n$) est susceptible d'être représenté par le système complet des formes de première (seconde) espèce, dont D est le déterminant."

*) J'ai eu devoir sur ce point m'écarter de la terminologie adoptée dans les *Disq. arithm.*, pour pouvoir conserver dans les dénominations l'analogie qui existe entre les objets qu'elles servent à désigner. Les formes quadratiques à coefficients complexes dont nous aurons à nous occuper dans la suite de ces recherches, présentent sous le rapport dont il s'agit ici, une variété plus grande que les formes ordinaires, et à laquelle les expressions employées par M. Gauss ne s'adapteraient que difficilement. En effet dans les formes de cette nature, le plus grand diviseur commun de a , $2b$, c peut être l'unité, le nombre $1 + \sqrt{-1}$, ou enfin le nombre 2, en supposant toujours celui de a , b , c égal à l'unité.

Il importe de remarquer que ce résultat présente les mêmes cas d'exception que le théorème I du §. 4, et que le nombre des représentations est respectivement pour ces deux cas 4σ ou 6σ .

En attribuant à D des valeurs déterminées, on obtient des théorèmes très simples tels que ceux-ci:

„Le nombre des solutions de l'équation $x^2 + y^2 = n$ est égal au quadruple de l'excès du nombre des diviseurs de n qui ont la forme $4\nu + 1$, sur celui des diviseurs compris dans la forme $4\nu + 3$.“

„Le nombre des solutions de l'équation $x^2 + 2y^2 = n$ est égal au double de l'excès des diviseurs de n , qui sont de l'une des formes $8\nu + 1$, 3 , sur celui de ces diviseurs qui sont de l'une de celles-ci: $8\nu + 5$, 7 .“

Et ainsi de suite.

Le premier de ces théorèmes particuliers était déjà connu. M. JACOBI qui l'avait d'abord conclu du rapprochement de deux séries qui appartiennent à la théorie des fonctions elliptiques, en a donné depuis une démonstration purement arithmétique*).

On peut, par des considérations du même genre, parvenir au résultat général énoncé ci-dessus en partant du théorème déjà cité du §. 4. C'est ce que nous allons faire voir en peu de mots en nous bornant au cas où les formes sont de la première espèce, le même raisonnement s'appliquant à l'autre cas. Supposons en premier lieu que les diviseurs simples de n soient tous de l'espèce de ceux que nous avons désignés par f , et posons $n = f_1^{\lambda_1} f_2^{\lambda_2} f_3^{\lambda_3} \dots f_1, f_2, f_3, \dots$ désignant des nombres premiers inégaux. Pour faire l'énumération complète de toutes les représentations dont n est susceptible, nous les rangerons en groupes, en comprenant dans le même groupe celles de ces représentations pour lesquelles le plus grand diviseur commun des indéterminées x et y a la même valeur l , dont le carré devra évidemment diviser n . Il est évident que le nombre des représentations contenues dans un pareil groupe, est le même que celui des représentations de l'entier $\frac{n}{l^2}$, en assujettissant les indéterminées x et y à être premières entre elles. Or il résulte de la supposition faite sur la nature de f_1, f_2, \dots et du théorème déjà cité, que ce dernier nombre est exprimé par 2.2^μ , μ désignant le nombre des diviseurs simples inégaux de $\frac{n}{l^2}$.

*) Voyez le Tome XII du Journal de CRELLE p. 167.

Tout se réduit donc à déterminer la somme des puissances 2^u qui correspondent aux entiers de la forme $\frac{n}{f^2}$. Pour obtenir cette somme, considérons le polynôme :

$$F_1 = 2f_1^{\lambda_1} + 2f_1^{\lambda_1-2} + 2f_1^{\lambda_1-4} + \dots$$

qui doit être continué tant que les exposants ne deviennent pas négatifs, et dans lequel le coefficient du dernier terme est supposé égal à 2 ou à 1, selon que l'exposant de ce terme a la valeur 1 ou 0. Le produit développé de ce polynôme et des polynômes analogues relatifs à f_2, f_3, \dots étant évidemment composé de tous les termes de la forme $2^u \frac{n}{f^2}$, on obtiendra la somme des puissances 2^u , en remplaçant les nombres f_1, f_2, \dots par l'unité. Mais par ce changement F_1, F_2, \dots deviendront respectivement $\lambda_1 + 1, \lambda_2 + 1, \dots$, d'où l'on conclut que le nombre des représentations qu'il s'agit d'obtenir, est égal au double du produit $(\lambda_1 + 1)(\lambda_2 + 1) \dots$ qui exprime, comme l'on sait, le nombre des diviseurs de n . On voit que dans ce premier cas, le résultat est conforme à l'énoncé général, puisque dans ce cas, où les diviseurs remplissent tous la première des deux conditions exprimées dans cet énoncé, le nombre des diviseurs ne diffère pas de l'excès désigné par σ . Passons maintenant au cas général où n renferme aussi des nombres premiers g , tels qu'on ait :

$$d^{\frac{1}{2}(\sigma-1)} \varepsilon^{\frac{1}{2}(\sigma-1)} \left(\frac{g}{P} \right) = -1,$$

et posons :

$$n = f_1^{\lambda_1} f_2^{\lambda_2} \dots \times g_1^{\nu_1} g_2^{\nu_2} \dots$$

Il est facile de conclure du cas déjà examiné que dans cette supposition le nombre des représentations dont n est susceptible, sera exprimé par $2(\lambda_1 + 1)(\lambda_2 + 1) \dots$, lorsque les exposants ν_1, ν_2, \dots sont tous pairs, et se réduit au contraire à zéro, lorsque cette circonstance n'a pas lieu. Nous avons donc à prouver que l'excès σ a la valeur $(\lambda_1 + 1)(\lambda_2 + 1) \dots$ ou la valeur zéro, selon que n se trouve dans le premier ou le second de ces deux cas. Pour y parvenir, faisons le produit des expressions :

$$1 + f_1 + \dots + f_1^{\lambda_1}, \quad 1 + f_2 + \dots + f_2^{\lambda_2}, \quad \dots, \quad 1 + g_1 + \dots + g_1^{\nu_1}, \quad 1 + g_2 + \dots + g_2^{\nu_2}, \quad \dots$$

dont les différents termes donnent tous les diviseurs de n . L'un quelconque de ces diviseurs étant désigné par k , on aura $d^{\frac{1}{2}(k-1)} \varepsilon^{\frac{1}{2}(k-1)} \left(\frac{k}{P} \right) = \pm 1$, le signe supérieur ou inférieur ayant lieu, selon que le nombre des facteurs g_1, g_2, \dots

contenus dans k sera pair ou impair. On conclut de là que le produit précédent se changera en σ , si l'on y fait $1 = f_1 = f_2 = \dots$, $-1 = g_1 = g_2 = \dots$. Le produit deviendra ainsi:

$$(\lambda_1 + 1)(\lambda_2 + 1) \dots \times \frac{1 - (-1)^{\nu_1 + 1}}{2} \cdot \frac{1 - (-1)^{\nu_2 + 1}}{2} \dots,$$

et il est évident que cette expression est en effet $(\lambda_1 + 1)(\lambda_2 + 1) \dots$, lorsque ν_1, ν_2, \dots sont tous pairs, et zéro dans tout autre cas.

Les résultats précédents sont relatifs au cas où le déterminant D est un entier négatif. Il existe des propriétés analogues pour les formes dont le déterminant est positif. Pour établir ces propriétés, on peut faire usage des séries que nous avons considérées dans les Nos. III et IV du §. 6. On peut aussi y parvenir par des raisonnements purement arithmétiques entièrement semblables à ceux que nous venons d'indiquer, et en prenant pour point de départ le théorème III du §. 4.

Il serait donc inutile d'entrer dans de nouveaux détails à cet égard, et nous nous bornerons à énoncer les résultats qui se rapportent aux formes à déterminant positif. Mais il est bon de faire précéder cet énoncé d'une remarque propre à le simplifier et qui concerne les conditions auxquelles les coefficients des formes à déterminant positif ont été assujetties dans les §§. 4 et 6. On y a supposé, que les coefficients de chacune de ces formes, telle que $ax^2 + 2bxy + cy^2$, étaient les deux premiers positifs, le troisième négatif. Or de ces conditions la première et la troisième sont seules nécessaires, et tout ce qui a été démontré dans les paragraphes cités, subsiste également lorsque b est négatif ou zéro. Nous n'avons en effet eu nulle part égard au signe du coefficient moyen, si ce n'est dans le No. III du §. 6, pour prouver que l'expression $ax^2 + 2bxy + cy^2$ est positive, lorsqu'on y suppose:

$$x > 0, \quad y > 0, \quad y \leq \frac{aU}{T - bU} x.$$

Mais il est facile de voir que ce résultat ne dépend pas non plus du signe de b . Pour s'en assurer, on remarquera que la dernière des inégalités précédentes peut se mettre sous la forme $(ax + by)U \geq yT$, d'où l'on conclut, le second membre étant positif, $(ax + by)^2 U^2 \geq y^2 T^2$. On a, d'un autre côté, $T^2 > DU^2$, et par suite en multipliant, $(ax + by)^2 > Dy^2$, ou ce qui revient au même, le coefficient a étant positif, $ax^2 + 2bxy + cy^2 > 0$; ce qu'il s'agissait de prouver.

En ayant égard à la remarque qui vient d'être faite, et désignant comme

précédemment par ω l'unité ou le nombre 2, selon qu'il s'agira de formes de première ou de seconde espèce, on pourra réunir les résultats dont il s'agit dans l'énoncé suivant.

„ D étant un entier positif (non-carré) et T et U désignant les plus petites valeurs positives de t et u (autres que ω et 0) qui satisfont à l'équation $t^2 - Dn^2 = \omega^2$, supposons que :

$$ax^2 + 2bxy + cy^2, \quad a'x^2 + 2b'xy + c'y^2, \quad \dots$$

soient les formes différentes de première (seconde) espèce, ayant le nombre D pour déterminant, ces formes étant tellement choisies que les coefficients de x^2 soient tous positifs, et ceux de y^2 tous négatifs: supposons encore que les indéterminées x et y ne doivent recevoir que des valeurs positives, et soient de plus assujetties dans la première de ces formes à la condition $y \leq \frac{aU}{T-bU}x$, et dans les autres à des conditions analogues. Cela étant et n désignant un entier positif, impair et premier à D , je dis que le nombre des représentations différentes dont ωn est susceptible au moyen des formes données, est égal à l'excès du nombre des diviseurs k de n , pour lesquels l'expression $\delta^{\frac{1}{2}(k-1)} \varepsilon^{\frac{1}{2}(k^2-1)} \binom{k}{P}$ a la valeur 1, sur celui de ces diviseurs qui donnent à la même expression la valeur -1 .⁴

Pour appliquer ce théorème à un cas particulier, soit $D = 2$. On a alors $\omega = 1$, $T = 3$, $U = 2$, $\delta = 1$, $\varepsilon = -1$, $P = 1$, et le système complet des formes se réduit à un seul terme, pour lequel nous pouvons prendre la forme $x^2 - 2y^2$. Le résultat relatif à ce cas est donc :

„Si dans l'équation $x^2 - 2y^2 = n$, où n est impair et positif, les indéterminées x et y ne sont susceptibles que de valeurs positives et en outre telles qu'on ait $3y \leq 2x$, le nombre des solutions de cette équation sera exprimé par l'excès du nombre des diviseurs de n qui ont l'une des formes $8\nu \pm 1$, sur celui de ces diviseurs qui sont de l'une de celles-ci: $8\nu \pm 5$.⁵

Comme dans l'équation (1) établie ci-dessus, de même que dans les trois équations analogues que pour abrégé nous nous sommes dispensés d'écrire, les deux membres sont égaux par groupes de termes, en ce sens que le terme unique qui résulte de la réunion de tous les termes particuliers du second membre, pour lesquels le produit nn' a une valeur déterminée, est identique à celui qui provient dans le premier de tous les termes particuliers pour lesquels

les formes quadratiques ont cette même valeur déterminée. on voit que la vérité de ces équations est indépendante de la forme particulière de la fonction qui y entre, et que cette fonction qui, dans ces équations telles qu'elles se sont présentées d'abord, est une puissance de l'exposant $-s$, peut être remplacée par une fonction entièrement arbitraire. Il viendra ainsi, en n'écrivant toujours que l'équation qui se rapporte au premier des quatre cas généraux :

$$(2) \quad \Sigma' q(ax^2+2bxy+cy^2) + \Sigma' q(a'x^2+2b'xy+c'y^2) + \dots = 2 \Sigma \delta^{\frac{1}{2}(n-1)} \varepsilon^{\frac{1}{2}(n^2-1)} \binom{n}{P} q(nn'),$$

les signes sommatoires ayant toujours la même signification. Il faut seulement ajouter que la fonction désignée par la caractéristique q doit être telle que les séries précédentes soient convergentes et du nombre de celles que nous avons appelées séries de première espèce. Cette condition se trouvera remplie, par exemple, si l'on suppose :

$$q(z) = q^z.$$

q étant une constante réelle ou imaginaire, dont la valeur numérique ou le module soit moindre que l'unité. Ce cas est surtout remarquable, en ce qu'il permet d'effectuer l'une des sommations dans le second membre et de transformer les séries doubles contenues dans le premier, en sommes de produits de séries simples, de sorte que l'équation exprime alors un rapport entre certaines séries simples qui sont précisément celles qui se présentent dans la théorie des fonctions elliptiques. La simplification dont nous parlons, n'a toutefois lieu que pour l'équation (2) et pour l'autre équation analogue qui se rapporte à une valeur négative de D ; elle ne s'étend pas au cas où le déterminant est positif. On peut bien, dans ce dernier cas, exécuter encore l'une des sommations indiquées dans le second membre, mais les conditions d'inégalité auxquelles sont assujetties celles relatives à x et y empêchent que les séries doubles en x et y ne soient transformées en produits de séries simples.

Comme les formules auxquelles on se trouve conduit par la réduction dont nous venons de parler, sont nouvelles et paraissent présenter quelque intérêt, nous indiquerons brièvement la manière dont on peut l'effectuer. L'équation (2), lorsqu'on y attribue à la fonction q la forme exponentielle, se change en celle-ci :

$$(3) \quad \Sigma' q^{ax^2+2bxy+cy^2} + \Sigma' q^{a'x^2+2b'xy+c'y^2} + \dots = 2 \Sigma \delta^{\frac{1}{2}(n-1)} \varepsilon^{\frac{1}{2}(n^2-1)} \binom{n}{P} q^{nn'}.$$

Dans le cas particulier où les coefficients moyens b, b', \dots sont tous égaux

à zéro, le premier membre se présente immédiatement comme la somme d'un nombre limité de produits de séries simples. Soit, par exemple, $D = -2$: il n'existe alors que la seule forme $x^2 + 2y^2$, et la somme $\Sigma' q^{x^2+2y^2}$, dans laquelle $x^2 + 2y^2$ ne doit recevoir que des valeurs impaires, devra s'étendre à tous les entiers impairs x , et à tous les entiers pairs ou impairs y . En réunissant les termes qui répondent à des valeurs opposées de x ou de y , le premier membre prendra la forme de ce produit:

$$2(q + q^{3^2} + q^{5^2} + \dots)(1 + 2q^2 + 2q^{2 \cdot 2^2} + 2q^{2 \cdot 3^2} + \dots).$$

Quant au second membre, comme l'on a $\delta = -1$, $\varepsilon = -1$, $P = -1$, il deviendra $2 \Sigma (-1)^{\frac{1}{2}(n-1) + \frac{1}{8}(n^2-1)} q^{nn'}$, le signe Σ s'étendant à toutes les valeurs positives et impaires de n et de n' . En effectuant la sommation par rapport à n' , on aura:

$$2 \Sigma (-1)^{\frac{1}{2}(n-1) + \frac{1}{8}(n^2-1)} \frac{q^n}{1 - q^{2n}}.$$

On a donc dans ce cas particulier l'équation:

$$(q + q^9 + q^{25} + \dots)(1 + 2q^2 + 2q^8 + 2q^{18} + \dots) = \frac{q}{1 - q^2} + \frac{q^3}{1 - q^6} - \frac{q^5}{1 - q^{10}} - \frac{q^7}{1 - q^{14}} + \dots,$$

facile à vérifier par les formules connues de la théorie des fonctions elliptiques.

Passons à un cas plus général et qui suffira pour montrer de quelle manière la réduction dont il est question, pourra être effectuée quelle que soit la valeur négative attribuée à D . Soit $D = -p$, p désignant un nombre premier $4\nu + 3$. Dans cette supposition on a $\delta = 1$, $\varepsilon = 1$, $P = -p$; le second membre deviendra donc, en mettant au lieu de $\left(\frac{n}{-p}\right)$ l'expression équivalente $\binom{n}{p}$:

$$2 \Sigma \binom{n}{p} q^{nn'}.$$

Comme n et n' doivent recevoir toutes les valeurs positives impaires et premières à p , l'expression précédente, en y effectuant la sommation relative à n' , se changera en:

$$(4) \quad 2 \Sigma \binom{n}{p} \frac{q^n}{1 - q^{2n}} - 2 \Sigma \binom{n}{p} \frac{q^{np}}{1 - q^{2np}}.$$

Considérons maintenant l'une des sommes contenues dans le premier membre de l'équation (3), la première par exemple. D'après ce que nous avons vu au §. 5, les valeurs simultanées que x et y doivent obtenir dans

cette somme, peuvent être distribuées en un certain nombre de systèmes de la forme $x = 2pu + a$, $y = 2pr + \gamma$, où a et γ sont des entiers déterminés et u et r des entiers indéterminés qui doivent prendre toutes les valeurs depuis $-\infty$ jusqu'à ∞ . On aura donc, pour la somme partielle qui répond à ce système, en mettant $ax^2 + 2bxy + cy^2$ sous la forme $\frac{1}{a}((ax + by)^2 + py^2)$:

$$\sum q^{\frac{1}{a}(2p(au+be)+aa+by)^2} \frac{p}{q^a(2pr+\gamma)^2}$$

Décomposons maintenant cette somme partielle à son tour en d'autres sommes, en écrivant successivement av , $av + 1$, \dots , $av + a - 1$ à la place de v . On aura ainsi pour l'une quelconque de ces nouvelles sommes partielles, dont le nombre est a , l'expression suivante qui se rapporte à la substitution de $av + \lambda$, et dans laquelle on a fait, pour abrégér, $2pb\lambda + aa + b\gamma = k$, $2p\lambda + \gamma = l$:

$$\sum q^{\frac{1}{a}(2pa(u+be)+k)^2} \frac{p}{q^a(2par+l)^2}$$

Or, si l'on considère maintenant la sommation relative à u comme devant être effectuée la première, rien n'empêche de remplacer $u + be$ par u , et le résultat prend la forme d'un produit de deux séries simples:

$$(5) \quad \sum q^{\frac{1}{a}(2pau+k)^2} \sum q^{\frac{p}{a}(2par+l)^2}$$

Il est d'ailleurs facile de voir que ces deux séries peuvent être réduites à la fonction si remarquable que M. JACOBI a introduite dans la théorie des fonctions elliptiques et qui a pour expression:

$$1 - q \cos 2x + 2q^2 \cos 4x - 2q^3 \cos 6x + \dots$$

D'un autre côté, on peut aussi réduire aux fonctions elliptiques les deux séries (4), en combinant les formules connues de cette théorie avec les belles expressions que M. GAUSS a données pour exprimer $\left(\frac{n}{p}\right)$ par une série finie de sinus ou de cosinus.

Les formules que l'on obtient ainsi, me paraissent surtout remarquables en ce que les produits de la forme (5), qui composent le premier membre, dépendent, quant à leur nombre et quant aux constantes a , k , l qu'ils renferment, du nombre et des coefficients des formes quadratiques différentes qui ont lieu pour le déterminant correspondant, et il y a lieu d'espérer qu'en approfondissant le rapprochement que nous venons d'indiquer, on parviendra à des résultats plus importants et qui pourront jeter un nouveau jour sur la nature des formes

quadratiques à déterminant négatif. C'est du moins la considération qui me détermine à proposer cet aperçu, tout incomplet qu'il est, à l'attention des géomètres.

§. 8.

Nous nous proposons dans ce paragraphe 1°. d'établir la relation très simple qui existe entre les nombres des formes de première et de seconde espèce qui répondent au même déterminant et 2°. d'examiner de quelle manière le nombre des formes d'un déterminant quelconque dépend de celui qui se rapporte à ce déterminant, divisé par le plus grand carré qu'il contient.

I. Soient h et h' respectivement les nombres des formes de première et de seconde espèce dont le déterminant D est un entier $4\nu+1$. Si nous supposons en premier lieu D négatif, l'équation (19) §. 6 donnera, en observant qu'on a $\delta = 1$, $\varepsilon = 1$:

$$h = \frac{2}{\pi} \sqrt{|D|} \zeta\left(\frac{n}{D}\right) \frac{1}{n}.$$

Il suffit de comparer cette expression aux équations (21), pour en conclure:

$$h = h', \quad D \equiv 1 \pmod{8}; \quad h = 3h', \quad D \equiv 5 \pmod{8}.$$

Il faut seulement ajouter que la seconde de ces équations est en défaut pour $D = -3$, et qu'on a alors $h = h'$.

II. Lorsque D est positif, la relation qui existe entre h et h' , résulte de la même manière de la comparaison des équations (23) et (24). Si l'on désigne par T , U et T' , U' , respectivement les plus petites valeurs positives qui satisfont aux équations:

$$(1) \quad t^2 - Du^2 = 1, \quad (2) \quad t'^2 - Du'^2 = 4,$$

la relation dont il s'agit, sera exprimée comme il suit:

$$h = h' \frac{\log \frac{1}{2}(T' + U'\sqrt{D})}{\log(T + U\sqrt{D})}, \quad D \equiv 1 \pmod{8};$$

$$h = 3h' \frac{\log \frac{1}{2}(T' + U'\sqrt{D})}{\log(T + U\sqrt{D})}, \quad D \equiv 5 \pmod{8}.$$

Pour réduire ce résultat à une forme plus simple, nous observerons que les solutions de l'équation (1) sont évidemment toutes comprises dans celles de l'équation (2); il suffit de considérer celles de ces dernières où t' et u' sont pairs et de poser $t = \frac{1}{2}t'$, $u = \frac{1}{2}u'$. Il résulte de là que si T' et U' sont pairs, on a $T = \frac{1}{2}T'$, $U = \frac{1}{2}U'$, et il est facile de voir que ce cas a toujours lieu

lorsque D est de la forme $8\nu + 1$, puisque dans cette supposition l'équation (2) ne saurait être satisfaite par des valeurs impaires de t' et u' . Reste à considérer le cas où D a la forme $8\nu + 5$, et où en même temps T' et U' sont impairs. Comme toutes les solutions positives de l'équation (2) sont données par la formule:

$$\frac{t'+u'\sqrt{D}}{2} = \left(\frac{T'+U'\sqrt{D}}{2} \right)^n,$$

où n est un entier positif, on conclut de la remarque faite plus haut que l'on obtiendra les valeurs T et U , en déterminant le plus petit exposant n pour lequel t' et u' sont pairs, et en posant ensuite $T = \frac{1}{2}t'$, $U = \frac{1}{2}u'$. Or il est facile de voir que cet exposant est le nombre 3: car en faisant $n = 2$, on trouve pour u' la valeur impaire $T'U'$, tandis que celle qui répond à $n = 3$, et qui est $\frac{1}{4}U'(3T'^2 + DU'^2)$, est évidemment paire. On a donc:

$$T+U\sqrt{D} = \left(\frac{T'+U'\sqrt{D}}{2} \right)^3.$$

En appliquant les résultats précédents aux deux équations données ci-dessus, on voit que, pour un déterminant de la forme $8\nu + 1$, on a toujours $h = h'$, et que lorsque D a la forme $8\nu + 5$, tout dépend des entiers T' et U' : selon que ces entiers seront pairs ou impairs, on aura $h = 3h'$ ou $h = h'$.

III. Venant à la seconde des questions énoncées ci-dessus, nous remarquerons d'abord qu'après avoir établi dans ce qui précède, le rapport qui a lieu entre les formes de première et de seconde espèce qui appartiennent au même déterminant, nous pouvons, dans la question qui nous reste à traiter, considérer les formes qu'il s'agit de comparer, quant à leur nombre, comme appartenant à la première espèce. Soient D et $D' = DS^2$ les deux déterminants, D n'ayant pas de facteur carré et S étant supposé positif, et désignons par h et h' les nombres des formes qui répondent respectivement à ces deux déterminants. Comme les quantités δ , ε , P sont évidemment les mêmes pour ces deux déterminants, si l'on suppose en premier lieu D négatif, on aura en vertu de l'équation (19) du §. 6:

$$h = \frac{2\sqrt{D_1}}{\pi} \Sigma \delta^{\frac{1}{2}(n-1)} \varepsilon^{\frac{1}{2}(n-1)} \left(\frac{n}{P} \right) \frac{1}{n}, \quad h' = \frac{2S\sqrt{D_1}}{\pi} \Sigma \delta^{\frac{1}{2}(n-1)} \varepsilon^{\frac{1}{2}(n-1)} \left(\frac{n}{P} \right) \frac{1}{n}.$$

Quoique les termes généraux des deux séries contenues dans ces expressions soient de même forme, ces séries ont néanmoins des valeurs différentes. En effet, dans la première équation la sommation doit s'étendre à tous les entiers n impairs et premiers à D , tandis que dans la seconde n ne doit

recevoir que des valeurs impaires et premières à D' . Pour découvrir la relation qui existe entre ces deux sommes, il faut se reporter à l'équation (6) du §. 6. Si l'on suppose dans cette équation $\theta = \delta$, $\eta = \varepsilon$, $P_2 = P$, $R_1 = 1$, on voit que les séries précédentes peuvent être considérées l'une et l'autre comme la limite vers laquelle converge le produit:

$$II \frac{1}{1 - \delta^{\frac{1}{2}(q-1)} \varepsilon^{\frac{1}{2}(q^2-1)} \left(\frac{q}{P}\right) \frac{1}{q^s}}$$

lorsque la variable s approche indéfiniment de l'unité; mais il y a cette différence que lorsqu'il s'agit de la première série, il faut exclure de ce produit tous les nombres premiers impairs et positifs q qui divisent D , tandis que pour obtenir la seconde série, il faut exclure tous ceux de ces nombres q qui divisent $D' = DS^2$. Il résulte de là que si l'on désigne par r, r', r'', \dots les nombres premiers impairs, positifs et inégaux, contenus dans D' , sans l'être dans D , le rapport de la première série à la seconde a pour expression:

$$II \frac{1}{1 - \delta^{\frac{1}{2}(r-1)} \varepsilon^{\frac{1}{2}(r^2-1)} \left(\frac{r}{P}\right) \frac{1}{r}}$$

le signe II s'étendant à toutes les valeurs de r qu'on vient de définir.

Au moyen de ce résultat, la comparaison des équations en h et h' donnera celle-ci:

$$h' = hSII \left(1 - \delta^{\frac{1}{2}(r-1)} \varepsilon^{\frac{1}{2}(r^2-1)} \left(\frac{r}{P}\right) \frac{1}{r}\right),$$

qui exprime la relation cherchée entre h et h' . On doit ajouter que cette équation ne s'applique pas au cas où $D = -1$, et qu'il faut dans ce cas doubler son premier membre.

IV. Le cas où D et D' sont positifs, étant susceptible d'une analyse toute semblable, nous nous bornerons à énoncer le résultat qui s'y rapporte. Si l'on désigne par T, U et T', U' les plus petites valeurs positives qui satisfont aux équations $t^2 - Du^2 = 1$, $t'^2 - D'u'^2 = 1$, le résultat dont il s'agit, sera:

$$h' = hS \frac{\log(T+U\sqrt{D})}{\log(T'+U'\sqrt{D'})} \left(1 - \delta^{\frac{1}{2}(r-1)} \varepsilon^{\frac{1}{2}(r^2-1)} \left(\frac{r}{P}\right) \frac{1}{r}\right),$$

où l'on peut remarquer que le facteur logarithmique équivaut évidemment à l'unité divisée par le plus petit exposant positif λ tel que le coefficient de \sqrt{D} dans la puissance $(T+U\sqrt{D})^\lambda$ développée soit divisible par S .

Nous observons, en finissant ce paragraphe et avant de nous occuper de la sommation mentionnée au commencement du précédent paragraphe, que les deux questions que nous venons de traiter, ont déjà été résolues dans l'ouvrage de M. GAUSS (art. 253—256), mais par d'autres moyens. Quant aux résultats, on trouve que ceux de l'illustre auteur, identiques aux nôtres dans le cas des déterminants négatifs, en diffèrent essentiellement et se présentent sous une forme plus compliquée, lorsque la comparaison qu'il s'agit de faire, doit porter sur des formes à déterminant positif.

§. 9.

La sommation qui nous reste à effectuer, peut être opérée par deux méthodes différentes, en s'aidant des formules remarquables que M. GAUSS a établies dans le beau Mémoire ayant pour titre „*Summatio quarundam serierum singularium.*“*) La première de ces méthodes est fondée sur certaines séries connues ordonnées suivant les sinus ou les cosinus des arcs multiples. En l'employant dans la note**) qui a précédé le présent Mémoire, nous avons déjà remarqué qu'elle s'applique, de la même manière et avec une facilité égale, à toutes les séries qui servent à exprimer le nombre des formes pour un déterminant quelconque, c'est-à-dire aux deux séries générales (19) et (23) du §. 6. Nous avons même ajouté que les séries de cette forme sont encore susceptibles d'être sommées par le même moyen, dans plusieurs cas différents de celui où l'exposant s de la puissance $\frac{1}{n^s}$, contenue dans le terme général, est égal à l'unité, ce qui était d'ailleurs évident. En effet, la méthode dont il s'agit, consistant à remplacer le facteur qui multiplie $\frac{1}{n^s}$, au moyen des formules de M. GAUSS par un nombre limité de termes de l'une des formes $\sin nx$, $\cos nx$, on voit que la série, après cette transformation, se trouve changée en une somme de suites trigonométriques dont chacune a pour terme général une expression telle que $\frac{\sin nx}{n^s}$ ou $\frac{\cos nx}{n^s}$, et peut par conséquent être sommée pour les mêmes valeurs de s , pour lesquelles D. BERNOULLI a donné les sommes de ces dernières.

La seconde méthode est fondée sur le procédé connu de l'intégration des fractions rationnelles. Les séries déjà citées (19) et (23) §. 6, coïncident

*) Gauss' Werke, Bd. II, S. 9. K.

**) Voyez le tome XVIII du Journal de CRELLE p. 259. 1)

1) S. 357 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

avec celles qui forment la seconde des trois classes de suites infinies que nous avons eu à distinguer dans le Mémoire sur la progression arithmétique, et nous avons déjà observé dans le Mémoire cité §. 10. que les séries de seconde et troisième classe peuvent être sommées par la méthode qui avait été expliquée en détail dans le §. 4 du même Mémoire. Les deux méthodes que nous venons de citer, sont l'une et l'autre d'une grande simplicité. La seconde étant celle qui se présente le plus naturellement, nous allons l'employer d'abord. Mais avant d'entreprendre ce calcul, il faut rappeler les formules de M. GAUSS. Voici une démonstration de ces expressions, fondée sur les mêmes principes dont j'ai déjà fait usage dans un précédent mémoire*), mais plus simple à quelques égards.

Désignant par $f(x)$ une fonction de x , que je suppose continue entre les limites $x = 0$ et $x = \pi$, si l'on pose:

$$\int_0^{\pi} f(x) \cos s x dx = c_s,$$

on aura, comme l'on sait:

$$c_0 + 2 \sum c_s \cos s x = \pi f(x).$$

le signe \sum s'étendant à tous les entiers depuis $s = 1$ jusqu'à $s = \infty$. Comme ce développement subsiste entre les limites $x = 0$ et $x = \pi$ inclusivement, on aura en particulier:

$$c_0 + 2 \sum c_s = \pi f(0).$$

Il est facile de voir comment cette équation doit être modifiée, lorsque les limites de l'intégrale c_s ont des valeurs quelconques. Considérons par exemple les limites 0 et $2h\pi$, h désignant un entier positif, et posons:

$$(1) \quad \int_0^{2h\pi} f(x) \cos s x dx = c_s,$$

la fonction étant toujours continue entre ces limites. L'intégrale précédente étant partagée en $2h$ intégrales partielles dont les limites sont:

$$0 \text{ et } \pi, \quad \pi \text{ et } 2\pi, \quad \dots, \quad (2h-1)\pi \text{ et } 2h\pi,$$

et toutes ces nouvelles intégrales étant ramenées à avoir pour limites communes 0 et π , le premier membre de l'équation (1) se changera en:

$$\int_0^{\pi} [f(x) + f(2\pi-x) + f(2\pi+x) + \dots + f(2(h-1)\pi-x) + f(2(h-1)\pi+x) + f(2h\pi-x)] \cos s x dx.$$

* S. 237 und S. 257 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

Cette expression de c_s ayant la même forme que celle donnée ci-dessus, on aura :

$$(2) \quad c_0 + 2 \sum_{s=1}^{\infty} c_s = \pi(f(0) + f(2h, \pi) + 2 \sum_{s=1}^{s=\frac{1}{2}n-1} f(2s\pi)),$$

le terme général c_s du premier membre étant donné par l'équation (1). Cela posé, considérons l'intégrale :

$$\int_{-z}^z \cos(x^2) dx = a,$$

a étant une quantité numérique. Posons dans cette intégrale $x = \frac{z}{2} \sqrt{\frac{n}{2\pi}}$, z désignant la nouvelle variable et n étant un entier positif divisible par 4. Il viendra ainsi :

$$\int_{-z}^z \cos\left(\frac{n}{8\pi} z^2\right) dz = 2a \sqrt{\frac{2\pi}{n}}.$$

Cette intégrale étant décomposée en une infinité d'autres ayant pour limites deux multiples consécutifs de 2π , tels que $2s\pi$ et $2(s+1)\pi$, et ces nouvelles intégrales étant ramenées à avoir les limites communes 0 et 2π par le changement de z en $2s\pi + z$, on aura :

$$\sum_0^{2\pi} \cos \frac{n}{8\pi} (2s\pi + z)^2 dz = 2a \sqrt{\frac{2\pi}{n}}.$$

le signe \sum s'étendant depuis $s = -\infty$ jusqu'à $s = \infty$.

En développant sous le signe cosinus, omettant le terme $\frac{1}{2} n s^2 \pi$, multiple de 2π , et réunissant les termes de la somme qui répondent à des valeurs opposées de s , il viendra :

$$\int_0^{2\pi} \cos\left(\frac{n}{8\pi} z^2\right) dz + 2 \sum_0^{2\pi} \cos\left(\frac{n}{8\pi} z^2\right) \cos\left(s \frac{n z}{2}\right) dz = 2a \sqrt{\frac{2\pi}{n}},$$

le signe \sum s'étendant depuis $s = 1$ jusqu'à $s = \infty$. Si maintenant l'on fait $nz = 2x$, on aura :

$$\int_0^{n\pi} \cos\left(\frac{x^2}{2n\pi}\right) dx + 2 \sum_0^{n\pi} \cos\left(\frac{x^2}{2n\pi}\right) \cos sx dx = a \sqrt{2n\pi}.$$

Comme l'entier n est pair, le premier membre rentre dans la forme de celui de l'équation (2), $f(x)$ étant $\cos\left(\frac{x^2}{2n\pi}\right)$. On aura donc en vertu de cette équation :

$$\cos 0 + \cos\left(\frac{n}{2}\right) \frac{2\pi}{n} + 2 \sum_{s=1}^{s=\frac{1}{2}n-1} \cos s^2 \frac{2\pi}{n} = a \sqrt{\frac{2n}{\pi}}.$$

Si l'on observe que l'on a $\cos s^2 \frac{2\pi}{n} = \cos(n-s)^2 \frac{2\pi}{n}$, l'équation précédente pourra prendre cette forme plus simple :

$$\sum_{s=0}^{s=n-1} \cos s^2 \frac{2\pi}{n} = a \sqrt{\frac{2n}{\pi}}.$$

Pour déterminer la quantité a indépendante de n , il suffira de donner à n une valeur particulière. Posant, par exemple, $n = 4$, on trouve $a = \sqrt{\frac{1}{2}}\pi$. On a donc définitivement, quel que soit l'entier $n = 4\mu$:

$$\sum_{s=0}^{s=n-1} \cos s^2 \frac{2\pi}{n} = \sqrt{n}.$$

En opérant de la même manière sur l'intégrale $\int_{-\infty}^{\infty} \sin(x^2) dx$, on trouve aussi :

$$\sum_{s=0}^{s=n-1} \sin s^2 \frac{2\pi}{n} = \sqrt{n}.$$

Il serait facile d'obtenir par une analyse semblable les sommes de la forme des précédentes, pour les cas où n est de l'une des trois formes $4\mu+1$, $4\mu+2$, $4\mu+3$; mais il est plus simple encore de ramener ces cas à celui où n a la forme 4μ .

Pour y parvenir, soient n et m deux entiers quelconques dont le premier est supposé positif, et posons :

$$\sum_{s=0}^{s=n-1} e^{s^2 \frac{2m\pi i}{n}} = q(m, n),$$

où i désigne, pour abrégé, la quantité imaginaire $\sqrt{-1}$.

La fonction $q(m, n)$ jouit de plusieurs propriétés remarquables. On a d'abord évidemment, si m' désigne un troisième entier tel qu'on ait $m' \equiv m \pmod{n}$:

$$(3) \quad q(m, n) = q(m', n).$$

On a encore, en supposant c premier à n :

$$(4) \quad q(m, n) = q(c^2 m, n).$$

Cela résulte de ce que l'expression cs , en y faisant successivement :

$$s = 0, 1, \dots, n-1,$$

donne les mêmes nombres pour restes lorsqu'on la divise par n .

Une troisième propriété est exprimée par l'équation :

$$(5) \quad q(m, n)q(n, m) = q(1, mn),$$

qui suppose les entiers n et m l'un et l'autre positifs et premiers entre eux.

En effet, comme on a :

$$\sum_{s=0}^{s=n-1} e^{s^2 \frac{2m\pi i}{n}} = g(m, n), \quad \sum_{t=0}^{t=m-1} e^{t^2 \frac{2n\pi i}{m}} = g(n, m),$$

il viendra en multipliant :

$$\Sigma \Sigma e^{\frac{(m^2 s^2 + n^2 t^2) 2\pi i}{mn}} = g(m, n)g(n, m),$$

ou encore, si l'on ajoute à l'exposant l'expression $2st\pi i$, multiple de $2\pi i$:

$$\Sigma \Sigma e^{\frac{(ms+nt)^2 2\pi i}{mn}} = g(m, n)g(n, m).$$

Le binôme $ms+nt$ peut être remplacé par son reste relatif au diviseur mn . Or, m et n étant premiers entre eux, il est facile de voir que les valeurs de ce reste entre les limites de la double sommation, coïncident, abstraction faite de l'ordre, avec les termes de la suite $0, 1, 2, \dots, mn-1$. Le résultat prend donc la forme d'une somme simple et l'on a :

$$\sum_{s=0}^{s=mn-1} e^{s^2 \frac{2\pi i}{mn}} = g(m, n)g(n, m),$$

ce qu'il s'agissait de prouver.

Au moyen des équations qui viennent d'être établies, il est facile d'obtenir la valeur de $g(1, n)$, quelle que soit la forme de l'entier n . Si l'on suppose d'abord $n = 4\mu$, on aura, en vertu des sommations effectuées plus haut :

$$g(1, n) = (1+i)\sqrt{n}.$$

Soit en second lieu n un entier impair. L'équation (5) donne, en y faisant $m = 4$:

$$g(4, n)g(n, 4) = g(1, 4n).$$

Le second membre est, d'après l'équation précédente, égal à $2(1+i)\sqrt{n}$. D'un autre côté, les deux expressions $g(4, n)$, $g(n, 4)$ peuvent, au moyen des équations (3) et (4), être remplacées, la première par $g(1, n)$, la seconde par $g(1, 4)$ ou par $g(3, 4)$, suivant que n est de la forme $4\mu+1$ ou de $4\mu+3$. Or il est facile de voir qu'on a :

$$g(1, 4) = 2(1+i), \quad g(3, 4) = 2(1-i).$$

On conclut de là :

$$g(1, n) = \sqrt{n}, \quad n = 4\mu+1; \quad g(1, n) = i\sqrt{n}, \quad n = 4\mu+3.$$

Reste à considérer le cas où n a la forme $4\mu+2$. Dans cette supposition, $\frac{n}{2}$ et 2 étant premiers entre eux, l'équation (5) donnera :

$$g\left(2, \frac{n}{2}\right) \cdot g\left(\frac{n}{2}, 2\right) = g(1, n),$$

et comme d'un autre côté, $g\left(\frac{n}{2}, 2\right) = g(1, 2) = 0$, il s'ensuivra :

$$g(1, n) = 0.$$

Considérons spécialement le cas où n est un nombre premier impair p , et soient a et b respectivement les résidus et les non-résidus quadratiques de p , moindres que ce nombre. On aura alors, en observant que l'expression $i^{\left(\frac{p-1}{2}\right)^2}$ se réduit à 1 ou à i , suivant que p a la forme $4u+1$ ou $4u+3$:

$$g(1, p) = i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p},$$

équation qu'on peut mettre, en remplaçant s^2 par son reste, sous cette forme :

$$1 + 2\Sigma e^{\frac{a \cdot 2\pi i}{p}} = i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p},$$

le signe Σ s'étendant à toutes les valeurs de a . Si m désigne un entier non-divisible par p , on aura pareillement, en remplaçant ms^2 par son reste :

$$g(m, p) = 1 + 2\Sigma e^{\frac{a \cdot 2\pi i}{p}} \quad \text{ou} \quad g(m, p) = 1 + 2\Sigma e^{\frac{b \cdot 2\pi i}{p}},$$

suivant que :

$$\left(\frac{m}{p}\right) = 1 \quad \text{ou} \quad \left(\frac{m}{p}\right) = -1.$$

Puisque d'un autre côté :

$$\Sigma e^{\frac{a \cdot 2\pi i}{p}} + \Sigma e^{\frac{b \cdot 2\pi i}{p}} = -1,$$

on pourra réunir les deux résultats dans cette formule :

$$g(m, p) = \left(\frac{m}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p}.$$

On donnera à l'expression $g(m, p)$, en y mettant au lieu de s^2 son reste, cette forme :

$$g(m, p) = 1 + 2\Sigma e^{\frac{a \cdot 2m\pi i}{p}}$$

et la comparaison de ces deux équations fournira celle-ci :

$$1 + 2\Sigma e^{\frac{a \cdot 2m\pi i}{p}} = \left(\frac{m}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p}.$$

Si maintenant l'on observe qu'on a évidemment $\Sigma e^{\frac{a \cdot 2m\pi i}{p}} + \Sigma e^{\frac{b \cdot 2m\pi i}{p}} = -1$, l'équation précédente pourra se changer en celle-ci :

$$1 + 2\Sigma e^{\frac{b \cdot 2m\pi i}{p}} = -\left(\frac{m}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p}.$$

En soustrayant cette équation de la précédente et divisant le résultat par 2, on aura définitivement:

$$\Sigma e^{a \frac{2m\tau i}{p}} - \Sigma e^{b \frac{2m\tau i}{p}} = \left(\frac{m}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} V \bar{p}.$$

Cette équation subsiste quel que soit l'entier m , pourvu qu'il ne soit pas divisible par p . Lorsque m est un multiple de p , le premier membre se réduit évidemment à zéro. Nous écrirons l'équation d'une manière plus abrégée et comme il suit:

$$(6) \quad \Sigma \left(\frac{g}{p}\right) e^{g \frac{2m\tau i}{p}} = \left(\frac{m}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} V \bar{p},$$

où le signe sommatoire s'étend depuis $g = 1$ jusqu'à $g = p - 1$.

§. 10.

D'après les résultats obtenus dans le §. 8, où nous avons fait voir que la détermination du nombre h des formes quadratiques qui répondent à un déterminant quelconque, se réduit toujours à une question du même genre et relative au cas où le déterminant n'a pas de diviseur carré et où les formes dont il s'agit d'obtenir le nombre, appartiennent à la première espèce, nous n'avons plus à nous occuper que des 4 déterminants:

$$P, \quad 2P, \quad -P, \quad -2P.$$

$P = pp'p'' \dots$ désignant un entier impair et positif dont les diviseurs simples p, p', p'', \dots sont tous différents les uns des autres.

Il importe de remarquer que la lettre P telle qu'on vient de la définir, a la même signification que dans les §§. 5 et 6, lorsque le déterminant que nous désignerons toujours par D , est positif, mais que dans le cas de D négatif, cette lettre telle qu'elle a été employée dans les paragraphes cités, répond à ce que nous désignons maintenant par $-P$. Cela ne change rien à l'expression $\left(\frac{n}{p}\right)$, contenue dans l'équation (19) du §. 6, et à la valeur de ε fixée par les équations (9) du même paragraphe, cette valeur devant être $+1$ ou -1 , suivant que le déterminant, délivré de tout diviseur carré, est impair ou pair. Mais il n'en est pas de même de δ , cette valeur dépendant du reste que donne P , pris avec son signe, relativement au diviseur 4. Il résulte de là qu'en posant pour abrégé:

$$V = \Sigma \delta^{\frac{1}{2}n-1} \varepsilon^{\frac{1}{2}n'-1} \left(\frac{n}{p}\right) \frac{1}{n}.$$

où le signe Σ s'étend à tous les entiers n positifs, impairs et premiers à P , les expressions $\delta = \pm 1$, $\varepsilon = \pm 1$ qui doivent entrer dans la série V contenue dans l'équation (19) ou (23), suivant qu'il s'agit d'un déterminant négatif ou positif, seront déterminées comme il suit:

$$\begin{aligned} \left. \begin{array}{l} D = P, \\ D = -P, \end{array} \right\} \begin{array}{l} P = 4\mu + 1 \\ P = 4\mu + 3 \end{array} \left. \vphantom{\begin{array}{l} D = P, \\ D = -P, \end{array}} \right\} \delta = 1, \quad \varepsilon = 1; \\ \left. \begin{array}{l} D = P, \\ D = -P, \end{array} \right\} \begin{array}{l} P = 4\mu + 3 \\ P = 4\mu + 1 \end{array} \left. \vphantom{\begin{array}{l} D = P, \\ D = -P, \end{array}} \right\} \delta = -1, \quad \varepsilon = 1; \\ \left. \begin{array}{l} D = 2P, \\ D = -2P, \end{array} \right\} \begin{array}{l} P = 4\mu + 1 \\ P = 4\mu + 3 \end{array} \left. \vphantom{\begin{array}{l} D = 2P, \\ D = -2P, \end{array}} \right\} \delta = 1, \quad \varepsilon = -1; \\ \left. \begin{array}{l} D = 2P, \\ D = -2P, \end{array} \right\} \begin{array}{l} P = 4\mu + 3 \\ P = 4\mu + 1 \end{array} \left. \vphantom{\begin{array}{l} D = 2P, \\ D = -2P, \end{array}} \right\} \delta = -1, \quad \varepsilon = -1. \end{aligned}$$

Cela posé, nous avons successivement à considérer les quatre combinaisons que présentent les équations simultanées $\delta = \pm 1$, $\varepsilon = \pm 1$.

I. Supposons d'abord $\delta = 1$, $\varepsilon = 1$. La série V étant divisée par $\left(1 - \left(\frac{2}{P}\right)\frac{1}{2}\right)$, il viendra:

$$\frac{V}{1 - \left(\frac{2}{P}\right)\frac{1}{2}} = \Sigma \left(\frac{n}{P}\right) \frac{1}{n},$$

le signe Σ s'étendant à tous les entiers positifs n , premiers à P , pairs ou impairs.

En exprimant la série par une intégrale comme au §. 1, on aura:

$$\frac{V}{1 - \left(\frac{2}{P}\right)\frac{1}{2}} = - \int_0^1 \frac{1}{x} \frac{f(x) dx}{x^P - 1},$$

où l'on a fait, pour abrégér, $f(x) = \Sigma \left(\frac{n}{P}\right) x^n$, le signe Σ s'étendant aux entiers précédemment définis moindres que P . En appliquant à cette intégrale la méthode ordinaire de décomposition, on trouve:

$$\frac{V}{1 - \left(\frac{2}{P}\right)\frac{1}{2}} = - \frac{1}{P} \Sigma f \left(e^{\frac{2m\pi i}{P}} \right) \int_0^1 \frac{dx}{x - e^{\frac{2m\pi i}{P}}},$$

le signe Σ s'étendant à tous les entiers m depuis $m = 0$ jusqu'à $m = P - 1$.

Tout se réduit donc à obtenir la fonction $f \left(e^{\frac{2m\pi i}{P}} \right) = \Sigma \left(\frac{n}{P} \right) e^{\frac{n}{P} 2m\pi i}$.

Pour y parvenir, mettons la fraction $\frac{n}{P}$, contenue dans l'exposant, sous la forme:

$$\frac{n}{P} = \mu + \frac{g}{p} + \frac{g'}{p'} + \dots,$$

μ étant un entier positif ou négatif, et g, g', \dots désignant des entiers positifs respectivement inférieurs à p, p', \dots . On sait que cela ne peut se faire que d'une seule manière (*Disq. arith.* 311), et il est manifeste, n étant premier à P , qu'aucun des entiers g, g', \dots ne saurait être zéro. Il est encore facile de voir qu'en donnant à n toutes les valeurs qu'il doit recevoir dans la sommation, g, g', \dots présenteront toutes les combinaisons que l'on peut former avec les entiers depuis $g = 1$ jusqu'à $g = p - 1$, depuis $g' = 1$ jusqu'à $g' = p' - 1$, etc. Quant à l'entier μ , on pourra le négliger parce qu'il est multiplié par $2m\pi i$ dans l'exposant. Si maintenant nous faisons pour un instant $\frac{P}{p} = r, \frac{P}{p'} = r', \dots$, l'équation précédente donne:

$$n \equiv gr + g'r' + \dots \pmod{P},$$

d'où l'on conclut ces égalités:

$$\left(\frac{n}{p}\right) = \left(\frac{g}{p}\right)\left(\frac{r}{p}\right), \quad \left(\frac{n}{p'}\right) = \left(\frac{g'}{p'}\right)\left(\frac{r'}{p'}\right), \quad \dots$$

au moyen desquelles la fonction $f\left(e^{\frac{2m\pi i}{P}}\right)$ deviendra le produit $\left(\frac{r}{p}\right)\left(\frac{r'}{p'}\right) \dots$ multiplié par les sommes:

$$\Sigma\left(\frac{g}{p}\right)e^{g\frac{2m\pi i}{p}}, \quad \Sigma\left(\frac{g'}{p'}\right)e^{g'\frac{2m\pi i}{p'}}, \quad \dots$$

Remplaçant ces dernières par leurs valeurs fournies par l'équation (6) du paragraphe précédent, on aura:

$$f\left(e^{\frac{2m\pi i}{P}}\right) = \left(\frac{r}{p}\right)\left(\frac{r'}{p'}\right) \dots i^{\left(\frac{p-1}{2}\right)^2 + \left(\frac{p'-1}{2}\right)^2 + \dots} \left(\frac{m}{P}\right) \sqrt{P}$$

en supposant m premier à P . Dans le cas contraire $f\left(e^{\frac{2m\pi i}{P}}\right)$ s'évanouira parce qu'une au moins des sommes précédentes se réduira à zéro. Quant au produit $\left(\frac{r}{p}\right)\left(\frac{r'}{p'}\right) \dots$, on remarquera qu'il se compose d'autant de produits partiels de la forme $\left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right)$, que les nombres p, p', \dots peuvent être combinés deux

à deux. Or, comme on a :

$$\left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right) = (-1)^{\frac{p-1}{2}\frac{p'-1}{2}} = i^{\frac{p-1}{2}\frac{p'-1}{2}},$$

on voit que l'expression qui multiplie $\left(\frac{m}{P}\right)\sqrt{P}$ dans l'équation obtenue plus haut, peut prendre la forme :

$$i^{\left(\frac{p-1}{2} + \frac{p'-1}{2} + \dots\right)^2} = i^{\left(\frac{P-1}{2}\right)^2}.$$

Nous avons donc définitivement :

$$(1) \quad f\left(e^{\frac{2m\pi i}{P}}\right) = 0 \quad \text{ou} \quad f\left(e^{\frac{2m\pi i}{P}}\right) = i^{\left(\frac{P-1}{2}\right)^2} \left(\frac{m}{P}\right)\sqrt{P},$$

suivant que m a ou n'a pas de diviseur commun avec P . Substituant cette valeur et observant que tant que $m < P$, on a :

$$\int_0^1 \frac{dx}{x - e^{\frac{2m\pi i}{P}}} = \log\left(2 \sin \frac{m\pi}{P}\right) + \frac{\pi}{2} \left(1 - \frac{2m}{P}\right) i,$$

il viendra :

$$\frac{V}{1 - \left(\frac{2}{P}\right)\frac{1}{2}} = -\frac{i^{\left(\frac{P-1}{2}\right)^2}}{\sqrt{P}} \Sigma\left(\frac{m}{P}\right) \left\{ \log\left(2 \sin \frac{m\pi}{P}\right) + \frac{\pi}{2} \left(1 - \frac{2m}{P}\right) i \right\},$$

le signe sommatoire s'étendant à tous les entiers m inférieurs et premiers à P . L'équation précédente se simplifie en remarquant qu'on a $\Sigma\left(\frac{m}{P}\right) = 0$; elle devient ainsi :

$$\frac{V}{1 - \left(\frac{2}{P}\right)\frac{1}{2}} = -\frac{i^{\left(\frac{P-1}{2}\right)^2}}{\sqrt{P}} \Sigma\left(\frac{m}{P}\right) \left(\log \sin \frac{m\pi}{P} - \frac{m\pi}{P} i \right).$$

Le premier membre étant réel, les imaginaires doivent se détruire dans le second, comme il est d'ailleurs facile de le vérifier.

Distinguons maintenant les deux formes que P peut présenter, en supposant successivement $P = 4\mu + 1$ et $P = 4\mu + 3$. Nous obtenons ainsi :

$$(a) \quad \begin{cases} P = 4\mu + 1, & V = -\frac{1}{\sqrt{P}} \left(1 - \left(\frac{2}{P}\right)\frac{1}{2}\right) \Sigma\left(\frac{m}{P}\right) \log \sin \frac{m\pi}{P}, \\ P = 4\mu + 3, & V = -\frac{\pi}{(\sqrt{P})^3} \left(1 - \left(\frac{2}{P}\right)\frac{1}{2}\right) \Sigma\left(\frac{m}{P}\right) m, \end{cases}$$

le signe Σ s'étendant toujours aux entiers m inférieurs et premiers à P .

II. Soit en second lieu $\delta = -1$, $\varepsilon = 1$. Comme le facteur qui multiplie $\frac{1}{n}$ dans la série V , est le même pour des valeurs de n qui diffèrent d'un multiple de $4P$, on aura d'après ce qui a été dit dans le §. 1:

$$V = - \int_0^1 \frac{1}{x} \frac{F(x) dx}{x^{4P} - 1},$$

en posant pour abrégér:

$$F(x) = \Sigma (-1)^{\frac{1}{2}(n-1)} \left(\frac{n}{P}\right) x^n,$$

le signe Σ s'étendant à tous les entiers n inférieurs et premiers à $4P$.

La méthode connue pour la décomposition des fractions rationnelles donne:

$$V = - \frac{1}{4P} \Sigma F \left(e^{\frac{2m\pi i}{4P}} \right) \int_0^1 \frac{dx}{x - e^{\frac{2m\pi i}{4P}}}.$$

où le signe Σ s'étend à tous les entiers depuis $m = 0$ jusqu'à $m = 4P - 1$.

Tout se réduit donc à déterminer l'expression $F \left(e^{\frac{2m\pi i}{4P}} \right)$.

On peut y parvenir par des considérations analogues à celles que nous avons employées dans le numéro précédent pour trouver $f \left(e^{\frac{2m\pi i}{P}} \right)$, mais il est plus simple de ramener ce cas à celui que nous avons déjà examiné. Pour cela, on décomposera la fraction $\frac{n}{4P}$, contenue dans l'exposant, comme il suit:

$$\frac{n}{4P} = \mu + \frac{\gamma}{4} + \frac{n'}{P}.$$

où il est facile de voir qu'en supposant γ et n' positifs et respectivement inférieurs à 4 et à P , les valeurs de γ et de n' présenteront, dans la sommation qu'il s'agit d'effectuer relativement à n , toutes les combinaisons des nombres γ inférieurs et premiers à 4, avec tous les nombres n' inférieurs et premiers à P . De l'équation précédente mise sous la forme:

$$n \equiv P\gamma + 4n' \pmod{4P},$$

on conclut facilement:

$$(-1)^{\frac{1}{2}(n-1)} = (-1)^{\frac{1}{2}(P-1)} (-1)^{\frac{1}{2}(\gamma-1)}, \quad \left(\frac{n}{P}\right) = \left(\frac{n'}{P}\right).$$

La fonction $F\left(e^{\frac{2m\pi i}{4P}}\right)$ deviendra par la substitution de ces valeurs:

$$F\left(e^{\frac{2m\pi i}{4P}}\right) = (-1)^{\frac{1}{2}(P-1)} \Sigma(-1)^{\frac{1}{2}(\gamma-1)} e^{\gamma \frac{2m\pi i}{4}} \cdot \Sigma\left(\frac{m'}{P}\right) e^{m' \frac{2m\pi i}{P}}.$$

Quant à la seconde des deux sommes contenues dans le second membre, elle est évidemment identique à la fonction $f\left(e^{\frac{2m\pi i}{P}}\right)$, n' ayant ici la même signification que n dans le numéro précédent. La première somme pourrait se déduire des formules données dans le §. 9, mais comme elle n'a que deux termes répondant à $\gamma = 1, 3$, on voit sans peine et indépendamment de ces formules que, pour une valeur impaire de m , elle se réduit à $2i(-1)^{\frac{1}{2}(m-1)}$, et qu'elle s'évanouit dans le cas contraire. Substituant les valeurs des deux sommes et remplaçant en même temps $(-1)^{\frac{1}{2}(P-1)}$ par $(i^2)^{\frac{1}{2}(P-1)}$, on aura:

$$(2) \quad F\left(e^{\frac{2m\pi i}{4P}}\right) = i^{\left(\frac{P+1}{2}\right)^2} (-1)^{\frac{1}{2}(m-1)} \left(\frac{m}{P}\right) \sqrt{4P}$$

en supposant m premier à $4P$. Dans le cas contraire le premier membre s'évanouit parce qu'au moins des sommes que nous venons de considérer, se réduit à zéro. Au moyen de ce résultat, on conclura:

$$V = -\frac{i^{\left(\frac{P+1}{2}\right)^2}}{\sqrt{4P}} \Sigma(-1)^{\frac{1}{2}(m-1)} \left(\frac{m}{P}\right) \left(\log 2 \sin \frac{m\pi}{4P} + i \frac{\pi}{2} \left(1 - \frac{m}{2P}\right)\right),$$

le signe s'étendant aux entiers m inférieurs et premiers à $4P$. Si l'on observe que pour ces valeurs on a:

$$\Sigma(-1)^{\frac{1}{2}(m-1)} \left(\frac{m}{P}\right) = 0,$$

l'équation précédente prendra la forme plus simple:

$$V = -\frac{i^{\left(\frac{P+1}{2}\right)^2}}{\sqrt{4P}} \Sigma(-1)^{\frac{1}{2}(m-1)} \left(\frac{m}{P}\right) \left(\log \sin \frac{m\pi}{4P} - i \pi \frac{m}{4P}\right).$$

En distinguant maintenant les deux formes que le nombre P peut présenter lorsqu'on le divise par 4, on aura:

$$(b) \quad \begin{cases} P = 4\mu + 3, & V = -\frac{1}{\sqrt{4P}} \Sigma(-1)^{\frac{1}{2}(m-1)} \left(\frac{m}{P}\right) \log \sin \frac{m\pi}{4P}, \\ P = 4\mu + 1, & V = -\frac{\pi}{(\sqrt{4P})^3} \Sigma(-1)^{\frac{1}{2}(m-1)} \left(\frac{m}{P}\right) m, \end{cases}$$

le signe sommatoire se rapportant aux entiers m inférieurs et premiers à $4P$.

III. Les cas qui nous restent à considérer et qui répondent à $\delta = 1$, $\varepsilon = -1$; $\delta = -1$, $\varepsilon = -1$, étant entièrement semblables à ceux qui viennent d'être traités, nous indiquerons rapidement le calcul qui s'y applique. En conservant d'abord la valeur ambiguë $\delta = \pm 1$, on aura :

$$V = - \int_0^1 \frac{1}{x} \frac{\Sigma \delta^{\frac{1}{2}(n-1)} (-1)^{\frac{1}{2}(n^2-1)} \left(\frac{n}{P}\right) x^n}{x^{8P}-1} dx,$$

le signe Σ s'étendant aux entiers n inférieurs et premiers à $8P$. On conclut de là :

$$V = - \frac{1}{8P} \Sigma A_m \int_0^1 \frac{dx}{x - e^{\frac{2m\pi i}{8P}}},$$

le signe Σ se rapportant aux entiers compris entre $m = 0$ et $m = 8P - 1$, et A_m désignant, pour abrégé, la somme :

$$\Sigma \delta^{\frac{1}{2}(n-1)} (-1)^{\frac{1}{2}(n^2-1)} \left(\frac{n}{P}\right) e^{\frac{n}{8P} 2m\pi i},$$

étendue aux entiers n définis plus haut. En faisant :

$$\frac{n}{8P} = \mu + \frac{\gamma}{8} + \frac{n'}{P},$$

il est facile de voir que n recevra toutes les valeurs auxquelles la sommation doit s'étendre, en combinant les entiers γ inférieurs et premiers à 8 avec les n' inférieurs et premiers à P . Si l'on remarque en outre qu'en vertu du §. 2, la congruence $n = P\gamma + 8n' \pmod{8P}$ entraîne ces équations :

$$\delta^{\frac{1}{2}(n-1)} = \delta^{\frac{1}{2}(P-1)} \delta^{\frac{1}{2}(\gamma-1)}, \quad (-1)^{\frac{1}{2}(n^2-1)} = (-1)^{\frac{1}{2}(P^2-1)} (-1)^{\frac{1}{2}(\gamma^2-1)},$$

$$\left(\frac{n}{P}\right) = \left(\frac{\gamma}{P}\right) \left(\frac{n'}{P}\right) = (-1)^{\frac{1}{2}(P^2-1)} \left(\frac{n'}{P}\right),$$

l'expression A_m prendra la forme :

$$A_m = \delta^{\frac{1}{2}(P-1)} f \left(e^{\frac{2m\pi i}{P}} \right) \Sigma \delta^{\frac{1}{2}(\gamma-1)} (-1)^{\frac{1}{2}(\gamma^2-1)} e^{\gamma \frac{2m\pi i}{8}}.$$

Tout se réduit donc à avoir la somme relative à γ . On pourrait la déduire du paragraphe précédent : mais comme elle ne se compose que d'un nombre limité de termes qui répondent à $\gamma = 1, 3, 5, 7$, on voit de suite que lorsqu'on a $\delta = 1$, la somme est zéro ou $(-1)^{\frac{1}{2}(m^2-1)} \sqrt{8}$, et que lorsqu'on a $\delta = -1$,

elle est zéro ou $(-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)}i\sqrt{8}$, suivant que m est pair ou impair. On conclut de là ces deux équations:

$$(3) \quad \Sigma(-1)^{\frac{1}{2}(m^2-1)}\left(\frac{n}{P}\right)e^{\frac{2m\pi i}{8P}} = (-1)^{\frac{1}{2}(m^2-1)}\left(\frac{m}{P}\right)i^{\left(\frac{P-1}{2}\right)^2}\sqrt{8P},$$

$$(4) \quad \Sigma(-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)}\left(\frac{n}{P}\right)e^{\frac{2m\pi i}{8P}} = (-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)}\left(\frac{m}{P}\right)i^{\left(\frac{P+1}{2}\right)^2}\sqrt{8P}.$$

qui supposent m premier à $8P$, et dont les seconds membres, dans le cas contraire, doivent être remplacés par zéro. Au moyen de ces expressions le calcul s'achève comme dans les cas déjà examinés, et l'on trouve:

$$(c) \quad \left. \begin{array}{l} \delta = 1, \quad \varepsilon = -1 \\ \delta = -1, \quad \varepsilon = -1 \end{array} \right\} \begin{cases} P = 4\mu + 1, & r = -\frac{1}{\sqrt{8P}} \Sigma(-1)^{\frac{1}{2}(m^2-1)}\left(\frac{m}{P}\right) \log \sin \frac{m\pi}{8P}, \\ P = 4\mu + 3, & r = -\frac{\pi}{(\sqrt{8P})^3} \Sigma(-1)^{\frac{1}{2}(m^2-1)}\left(\frac{m}{P}\right) m, \\ P = 4\mu + 3, & r = -\frac{1}{\sqrt{8P}} \Sigma(-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)}\left(\frac{m}{P}\right) \log \sin \frac{m\pi}{8P}, \\ P = 4\mu + 1, & r = -\frac{\pi}{(\sqrt{8P})^3} \Sigma(-1)^{\frac{1}{2}(m-1)+\frac{1}{8}(m^2-1)}\left(\frac{m}{P}\right) m. \end{cases}$$

les sommations s'étendant aux entiers m inférieurs et premiers à $8P$.

IV. Nous allons maintenant résoudre la question dont nous venons de nous occuper, par la première des deux méthodes indiquées plus haut, qui est celle des séries trigonométriques, en nous bornant toutefois, pour abrégé, aux séries r qui se rapportent aux déterminants négatifs.

Soit en premier lieu $\delta = 1, \varepsilon = 1, P = 4\mu + 3$; on a alors:

$$r = \Sigma \left(\frac{n}{P}\right) \frac{1}{n}.$$

le signe Σ se rapportant aux entiers n impairs et premiers à P . D'après l'équation (1), on a pour un nombre P de la forme $4\mu + 3$:

$$\frac{1}{\sqrt{P}} \Sigma \left(\frac{m}{P}\right) \sin n \frac{2m\pi}{P} = \left(\frac{n}{P}\right) \quad \text{ou} \quad = 0,$$

suivant que n est ou n'est pas premier à P , le signe Σ s'étendant aux entiers m inférieurs et premiers à P . Si l'on introduit cette expression dans la série r à la place de $\left(\frac{n}{P}\right)$, on pourra étendre la sommation relative à n à tous les entiers impairs, l'expression précédente s'évanouissant pour des valeurs de

n qui ne sont pas premières à P . Il viendra ainsi, en intervertissant l'ordre des deux sommes :

$$V = \frac{1}{\sqrt{P}} \Sigma \binom{m}{P} \Sigma \frac{1}{n} \sin n \frac{2m\pi}{P}.$$

La première peut s'obtenir au moyen du résultat connu d'après lequel la série :

$$(5) \quad \frac{\sin x}{1} + \frac{\sin 3x}{3} + \frac{\sin 5x}{5} + \dots$$

a la valeur $\frac{\pi}{4}$ ou $-\frac{\pi}{4}$, suivant que x est compris entre 0 et π , ou entre π et 2π . En distinguant donc les valeurs de m inférieures à $\frac{1}{2}P$ de celles qui surpassent $\frac{1}{2}P$, et désignant ces valeurs respectivement par m' et m'' , il viendra :

$$V = \frac{\pi}{4\sqrt{P}} \left(\Sigma \binom{m'}{P} - \Sigma \binom{m''}{P} \right).$$

Comme dans la seconde somme on peut évidemment remplacer m'' par $P-m'$, et qu'on a d'ailleurs, P étant de la forme $4\mu+3$:

$$\binom{P-m'}{P} = \binom{-1}{P} \binom{m'}{P} = - \binom{m'}{P},$$

on aura :

$$V = \frac{\pi}{2\sqrt{P}} \Sigma \binom{m'}{P},$$

expression d'une forme différente de celle que nous avons trouvée plus haut.

Si, avant de sommer, on avait divisé par $\left(1 - \left(\frac{2}{P}\right)\frac{1}{2}\right)$, on serait tombé sur le même résultat que nous avons obtenu par l'autre méthode.

Soit en second lieu $\delta = -1$, $\epsilon = 1$, $P = 4\mu+1$. On a alors :

$$V = \Sigma (-1)^{\frac{1}{2}(n-1)} \binom{n}{P} \frac{1}{n},$$

où n ne doit recevoir que des valeurs premières à $4P$. L'équation (2) donne pour ce cas :

$$\frac{1}{\sqrt{4P}} \Sigma (-1)^{\frac{1}{2}(n-1)} \binom{m}{P} \sin n \frac{2m\pi}{4P} = (-1)^{\frac{1}{2}(n-1)} \binom{n}{P} \quad \text{ou} \quad = 0,$$

suivant que n est ou n'est pas premier à $4P$, le signe Σ s'étendant aux entiers m inférieurs et premiers à $4P$. Introduisant cette expression dans la série V ,

il viendra :

$$\Gamma = \frac{1}{\sqrt{4P}} \Sigma (-1)^{\frac{1}{2}(m-1)} \binom{m}{P} \Sigma \frac{1}{n} \sin n \frac{2m\pi}{4P}.$$

L'expression qu'on a substituée, s'évanouissant lorsque n n'est pas premier à $4P$, on voit que l'on peut, dans la somme :

$$\Sigma \frac{1}{n} \sin n \frac{2m\pi}{4P}.$$

supposer à volonté que n obtient toutes les valeurs entières ou seulement celles qui sont impaires.

Dans la première supposition on aura en vertu de l'équation :

$$\frac{1}{2}(\pi - x) = \frac{\sin x}{1} + \frac{\sin 2x}{2} + \frac{\sin 3x}{3} + \dots$$

qui subsiste depuis $x = 0$ jusqu'à $x = 2\pi$:

$$\Sigma \frac{1}{n} \sin n \frac{2m\pi}{4P} = \frac{1}{2} \left(\pi - \frac{m\pi}{2P} \right).$$

et par suite :

$$\Gamma = \frac{\pi}{2\sqrt{4P}} \Sigma (-1)^{\frac{1}{2}(m-1)} \binom{m}{P} - \frac{\pi}{(\sqrt{4P})^3} \Sigma (-1)^{\frac{1}{2}(m-1)} \binom{m}{P} m,$$

ou ce qui revient au même, la première somme étant évidemment nulle :

$$\Gamma = -\frac{\pi}{(\sqrt{4P})^3} \Sigma (-1)^{\frac{1}{2}(m-1)} \binom{m}{P} m,$$

ce qui coïncide avec la valeur obtenue par l'autre méthode.

Si en second lieu on suppose que n ne reçoit que des valeurs impaires, on trouvera, au moyen de l'équation (5), et en désignant par m' ou m'' les valeurs de m , suivant qu'elles sont inférieures ou supérieures à $2P$:

$$\Gamma = \frac{\pi}{4\sqrt{4P}} \left(\Sigma (-1)^{\frac{1}{2}(m'-1)} \binom{m'}{P} - \Sigma (-1)^{\frac{1}{2}(m''-1)} \binom{m''}{P} \right).$$

En mettant $4P - m'$ à la place de m'' , et observant qu'on a :

$$(-1)^{\frac{1}{2}(4P-m'-1)} \binom{4P-m'}{P} = -(-1)^{\frac{1}{2}(m'-1)} \binom{m'}{P},$$

on obtiendra cette nouvelle expression de Γ :

$$\Gamma = \frac{\pi}{2\sqrt{4P}} \Sigma (-1)^{\frac{1}{2}(m'-1)} \binom{m'}{P}.$$

En traitant les deux autres cas de la même manière, on trouvera, outre les résultats déjà obtenus par l'autre méthode, deux nouveaux résultats que nous allons réunir avec les deux précédents:

$$(d) \begin{cases} \delta = 1, & \varepsilon = 1, & P = 4\mu + 3, & V = \frac{\pi}{2\sqrt{P}} \Sigma \left(\frac{m'}{P} \right), \\ \delta = -1, & \varepsilon = 1, & P = 4\mu + 1, & V = \frac{\pi}{2\sqrt{4P}} \Sigma (-1)^{\frac{1}{2}(m'-1)} \left(\frac{m'}{P} \right), \\ \delta = 1, & \varepsilon = -1, & P = 4\mu + 3, & V = \frac{\pi}{2\sqrt{8P}} \Sigma (-1)^{\frac{1}{2}(m'-1)} \left(\frac{m'}{P} \right), \\ \delta = -1, & \varepsilon = -1, & P = 4\mu + 1, & V = \frac{\pi}{2\sqrt{8P}} \Sigma (-1)^{\frac{1}{2}(m'-1) + \frac{1}{2}(m'-1)} \left(\frac{m'}{P} \right). \end{cases}$$

Les valeurs m' sont premières à P et en outre impaires dans les trois dernières équations. Quant aux limites des sommations, on doit ajouter que les valeurs de m' doivent être respectivement inférieures à $\frac{1}{2}P$, $2P$, $4P$, $4P$.

Les expressions de V peuvent prendre beaucoup d'autres formes encore. On obtient, par exemple, des expressions différentes des précédentes et plus simples, si dans le cas où le terme général renferme l'un des facteurs:

$$(-1)^{\frac{1}{2}(n-1)}, \quad (-1)^{\frac{1}{2}(n'-1)},$$

ou l'un et l'autre, on les conserve dans la série, en n'introduisant les formules de M. GAUSS que pour remplacer l'expression $\left(\frac{n}{P} \right)$. C'est ce que nous allons faire pour les trois derniers cas du tableau précédent (d).

Dans le premier de ces trois cas, on a:

$$V = \Sigma (-1)^{\frac{1}{2}(n-1)} \left(\frac{n}{P} \right) \frac{1}{n}, \quad P = 4\mu + 1.$$

et l'équation (1) donne alors:

$$\Sigma \left(\frac{m}{P} \right) \cos n \frac{2m\pi}{P} = \left(\frac{n}{P} \right) \sqrt{P} \quad \text{ou} \quad = 0,$$

suivant que n est ou n'est pas premier à P , m devant recevoir toutes les valeurs inférieures et premières à P . En substituant cette expression de $\left(\frac{n}{P} \right)$, on aura:

$$V = \frac{1}{\sqrt{P}} \Sigma \left(\frac{m}{P} \right) \Sigma (-1)^{\frac{1}{2}(n-1)} \frac{1}{n} \cos n \frac{2m\pi}{P},$$

où la sommation relative à n , peut maintenant s'étendre à tous les entiers impairs. Or on sait que la série:

$$\frac{\cos x}{1} - \frac{\cos 3x}{3} + \frac{\cos 5x}{5} - \dots$$

a la valeur:

$$\frac{\pi}{4}, \quad -\frac{\pi}{4}, \quad \frac{\pi}{4},$$

suivant que x est compris dans les trois intervalles:

$$0 \text{ et } \frac{\pi}{2}, \quad \frac{\pi}{2} \text{ et } \frac{3\pi}{2}, \quad \frac{3\pi}{2} \text{ et } 2\pi.$$

Désignant donc respectivement par m' , m'' , m''' les valeurs de m comprises dans les trois intervalles:

$$0 \text{ et } \frac{1}{4}P, \quad \frac{1}{4}P \text{ et } \frac{3}{4}P, \quad \frac{3}{4}P \text{ et } P,$$

on aura:

$$V = \frac{\pi}{4\sqrt{P}} \left[\Sigma \left(\frac{m'}{P} \right) - \Sigma \left(\frac{m''}{P} \right) + \Sigma \left(\frac{m'''}{P} \right) \right].$$

On a d'ailleurs évidemment:

$$\Sigma \left(\frac{m'}{P} \right) = \Sigma \left(\frac{m'''}{P} \right) \quad \text{et} \quad \Sigma \left(\frac{m'}{P} \right) + \Sigma \left(\frac{m''}{P} \right) + \Sigma \left(\frac{m'''}{P} \right) = 0.$$

d'où l'on conclut:

$$(e) \quad V = \frac{\pi}{\sqrt{P}} \Sigma \left(\frac{m'}{P} \right).$$

m' désignant les valeurs premières à P , comprises entre 0 et $\frac{1}{4}P$.

Dans le second cas on a:

$$V = \Sigma (-1)^{\frac{1}{2}(n^2-1)} \binom{n}{P} \frac{1}{n}. \quad P = 4\mu + 3.$$

En substituant la valeur de $\binom{n}{P}$ donnée par l'équation (1), il viendra:

$$V = \frac{1}{\sqrt{P}} \Sigma \left(\frac{m}{P} \right) \Sigma (-1)^{\frac{1}{2}(n^2-1)} \frac{1}{n} \sin n \frac{2m\pi}{P},$$

n pouvant maintenant recevoir toutes les valeurs impaires premières à P ou

non. Or la série:

$$\frac{\sin x}{1} - \frac{\sin 3x}{3} + \frac{\sin 5x}{5} - \frac{\sin 7x}{7} + \dots$$

étant sommée par les moyens connus, on trouve que sa valeur est respectivement:

$$0, \quad \frac{\pi}{2\sqrt{2}}, \quad 0, \quad -\frac{\pi}{2\sqrt{2}}, \quad 0.$$

suivant que x est compris dans les cinq intervalles:

$$0 \text{ et } \frac{\pi}{4}, \quad \frac{\pi}{4} \text{ et } \frac{3\pi}{4}, \quad \frac{3\pi}{4} \text{ et } \frac{5\pi}{4}, \quad \frac{5\pi}{4} \text{ et } \frac{7\pi}{4}, \quad \frac{7\pi}{4} \text{ et } 2\pi.$$

En désignant donc par m' les valeurs de m comprises entre $\frac{1}{3}P$ et $\frac{2}{3}P$, et par m'' celles qui tombent entre $\frac{2}{3}P$ et $\frac{1}{3}P$, on aura:

$$V = \frac{\pi}{2\sqrt{2}P} \left[\Sigma\left(\frac{m'}{P}\right) - \Sigma\left(\frac{m''}{P}\right) \right],$$

ou plus simplement en observant qu'on peut remplacer m'' par $P - m'$, et qu'on a

$$\left(\frac{P-m'}{P}\right) = -\left(\frac{m'}{P}\right):$$

$$(f) \quad V = \frac{\pi}{\sqrt{2}P} \Sigma\left(\frac{m'}{P}\right).$$

On trouve d'une manière semblable, P étant de la forme $4u + 1$:

$$(g) \quad V = \Sigma(-1)^{\frac{1}{2}(n-1) + \frac{1}{4}(n^2-1)} \left(\frac{n}{P}\right) \frac{1}{n} = \frac{\pi}{\sqrt{2}P} \left(\Sigma\left(\frac{m'}{P}\right) - \Sigma\left(\frac{m''}{P}\right) \right),$$

en désignant par m' et m'' les valeurs premières à P et respectivement comprises dans les deux intervalles 0 et $\frac{1}{3}P$, $\frac{2}{3}P$ et $\frac{1}{2}P$. Il importe de remarquer que les équations (e) et (g) ne s'appliquent pas au cas où $P = 1$.

§. 11.

On pourrait donner beaucoup d'autres formes à l'expression de la série V , soit que cette série réponde à un déterminant négatif, soit qu'elle se rapporte à un déterminant positif. Mais comme ces détails ne présentent aucune difficulté, nous ne nous y arrêterons pas et nous passons à l'énumération des différents théorèmes, qui résultent des équations (19) et (23) du §. 6, lorsqu'on y introduit les expressions qui viennent d'être obtenues.

Déterminants positifs.

$$(I) \quad D = P, \quad P = 4\mu + 1, \quad h = \frac{2 - \left(\frac{2}{P}\right)}{\log(T + U\sqrt{P})} \log \frac{H \sin \frac{b\pi}{P}}{H \sin \frac{a\pi}{P}},$$

où les entiers m inférieurs et premiers à P sont désignés par a ou par b , suivant que l'équation $\left(\frac{m}{P}\right) = \pm 1$ a lieu avec le signe supérieur ou avec le signe inférieur.

$$(II) \quad D = P, \quad P = 4\mu + 3, \quad h = \frac{1}{\log(T + U\sqrt{P})} \log \frac{H \sin \frac{b\pi}{4P}}{H \sin \frac{a\pi}{4P}},$$

où les entiers m inférieurs et premiers à $4P$ sont désignés par a ou par b , suivant que le signe ambigu, dans l'équation $(-1)^{\frac{1}{2}(m-1)} \left(\frac{m}{P}\right) = \pm 1$, est le signe supérieur ou inférieur.

$$(III) \quad D = 2P, \quad P = 4\mu + 1, \quad h = \frac{1}{\log(T + U\sqrt{2P})} \log \frac{H \sin \frac{b\pi}{8P}}{H \sin \frac{a\pi}{8P}},$$

où les entiers m inférieurs et premiers à $8P$ sont désignés par a ou par b , suivant que le signe ambigu, dans l'équation $(-1)^{\frac{1}{2}(m^2-1)} \left(\frac{m}{P}\right) = \pm 1$, est le signe supérieur ou inférieur.

$$(IV) \quad D = 2P, \quad P = 4\mu + 3, \quad h = \frac{1}{\log(T + U\sqrt{2P})} \log \frac{H \sin \frac{b\pi}{8P}}{H \sin \frac{a\pi}{8P}},$$

où les entiers m inférieurs et premiers à $8P$ sont désignés par a ou par b , suivant que l'on a $(-1)^{\frac{1}{2}(m-1) + \frac{1}{2}(m^2-1)} \left(\frac{m}{P}\right) = +1$ ou $= -1$.

Déterminants négatifs.

$$(V) \quad D = -P, \quad P = 4\mu + 3, \quad h = \left(2 - \left(\frac{2}{P}\right)\right) \frac{\Sigma b - \Sigma a}{P} = A - B.$$

Dans cette équation a et b ont la même signification que dans le premier cas, et A et B désignent respectivement combien il existe de valeurs a et b au-dessous de $\frac{1}{2}P$.

$$(VI) \quad D = -P; \quad P = 4\mu + 1. \quad h = \frac{\Sigma b - \Sigma a}{4P} = \frac{A - B}{2}.$$

Les lettres a et b ont la même signification que dans le second cas, et A et B désignent respectivement les nombres des valeurs a et b qui sont inférieures à $2P$. On a encore dans ce sixième cas, en désignant par A' et B' les nombres des valeurs a et b au-dessous de $\frac{1}{4}P$, a et b ayant le même sens que dans le premier cas :

$$h = 2(A' - B').$$

$$(VII) \quad D = -2P. \quad P = 4\mu + 3, \quad h = \frac{\Sigma b - \Sigma a}{8P} = \frac{A - B}{2}.$$

Les lettres a et b ont la même signification que dans le troisième cas, et A et B désignent respectivement les nombres des valeurs a et b moindres que $4P$. On a encore dans ce septième cas, en désignant par A' et B' les nombres des valeurs a et b , comprises entre $\frac{1}{8}P$ et $\frac{3}{8}P$, a et b ayant le même sens que dans le premier cas :

$$h = 2(A' - B').$$

$$(VIII) \quad D = -2P. \quad P = 4\mu + 1, \quad h = \frac{\Sigma b - \Sigma a}{8P} = \frac{A - B}{2}.$$

où a et b ont le même sens que dans le quatrième cas, et A et B désignent les nombres des valeurs a et b qui tombent au-dessous de $4P$. On a encore si, conservant aux lettres a et b la même signification que dans le premier cas, l'on désigne par A' , B' et A'' , B'' les nombres des valeurs a , b qui sont contenues dans les deux intervalles compris entre 0 et $\frac{1}{5}P$, $\frac{2}{5}P$ et $\frac{1}{2}P$:

$$h = 2(A' - B' - A'' + B'').$$

Il nous reste à présenter quelques remarques sur les résultats qui viennent d'être énoncés. Pour parler d'abord des quatre premiers cas, nous devons dire que les expressions qui s'y rapportent, quoique très simples, ne sont pas sous la forme qui en montre la véritable signification. Pour leur donner cette forme, nous nous occuperons spécialement du premier de ces cas. Les trois autres donnent lieu à des remarques entièrement semblables. Soit x une indéterminée et considérons les deux produits :

$$\Pi \left(x - e^{\frac{2a\pi i}{P}} \right), \quad \Pi \left(x - e^{\frac{2b\pi i}{P}} \right).$$

Il est évident qu'en posant :

$$X = H\left(x - e^{\frac{2a\pi i}{P}}\right) H\left(x - e^{\frac{2b\pi i}{P}}\right),$$

le polynôme X ne sera autre chose que le premier membre de l'équation que l'on obtient en dérivant l'équation binôme $x^P - 1 = 0$ de ses racines non-primitives. Il est facile de conclure de là que pour $x = 1$, on a :

$$X = 1 \quad \text{ou} \quad X = P$$

suivant que le nombre des facteurs simples p, p', p'', \dots de P est supérieur ou égal à l'unité. (Le cas où l'on aurait $P = 1$, est exclu, le déterminant étant un carré dans ce cas.)

On a donc suivant les deux cas qui viennent d'être distingués :

$$H\left(1 - e^{\frac{2a\pi i}{P}}\right) H\left(1 - e^{\frac{2b\pi i}{P}}\right) = 1 \quad \text{ou} \quad = P.$$

On a aussi :

$$H\left(1 - e^{\frac{2a\pi i}{P}}\right) = H\left(-2i \sin \frac{a\pi}{P}\right) e^{\frac{\pi i}{P} \Sigma a},$$

$$H\left(1 - e^{\frac{2b\pi i}{P}}\right) = H\left(-2i \sin \frac{b\pi}{P}\right) e^{\frac{\pi i}{P} \Sigma b};$$

observant donc que les valeurs a et b sont en nombre égal, que la suite des valeurs a renferme toujours avec un nombre a son complément $P - a$, et qu'il en est de même de la suite des valeurs b , on en conclura :

$$\frac{H \sin \frac{b\pi}{P}}{H \sin \frac{a\pi}{P}} = \frac{H\left(1 - e^{\frac{2b\pi i}{P}}\right)}{H\left(1 - e^{\frac{2a\pi i}{P}}\right)},$$

puis, en ayant égard à une équation précédente :

$$\frac{H \sin \frac{b\pi}{P}}{H \sin \frac{a\pi}{P}} = H\left(1 - e^{\frac{2b\pi i}{P}}\right)^2 \quad \text{ou} \quad = \frac{1}{P} H\left(1 - e^{\frac{2b\pi i}{P}}\right)^2$$

suivant les deux cas déjà distingués. La détermination de h dépend donc du produit :

$$H\left(1 - e^{\frac{2b\pi i}{P}}\right).$$

Or il résulte d'un théorème connu dû à M. GAUSS et qu'il est facile d'étendre à un nombre composé P , que le polynôme :

$$H\left(x - e^{\frac{2\theta\pi i}{P}}\right)$$

est toujours de la forme $\frac{1}{2}(Y+Z\sqrt{P})$, Y et Z étant des polynômes à coefficients entiers. En désignant donc par Y_1 et Z_1 les valeurs que Y et Z prennent pour $x = 1$, et passant des logarithmes aux nombres, l'équation qui détermine h , deviendra :

$$(T+U\sqrt{P})^h = \left(\frac{Y_1+Z_1\sqrt{P}}{2}\right)^{4-2\left(\frac{2}{P}\right)} \quad \text{ou} \quad (T+U\sqrt{P})^h = \left(\frac{Y_1+Z_1\sqrt{P}}{2\sqrt{P}}\right)^{4-2\left(\frac{2}{P}\right)},$$

suivant que le nombre des facteurs simples de P est supérieur ou égal à l'unité.

Sous cette forme les résultats qui se rapportent à un déterminant positif, paraîtront bien remarquables, s'il est vrai, comme l'a dit un illustre géomètre, que l'intérêt que présentent les recherches arithmétiques ait sa source non seulement dans la difficulté de la matière, mais surtout dans les rapports intimes que les recherches de ce genre dévoilent entre des théories entre lesquelles on ne soupçonnerait aucune connexion.

Quant au calcul des polynômes Y et Z , il peut se faire, soit par la méthode de M. GAUSS, soit par un moyen dont LEGENDRE a fait usage et qui est fondé sur les relations connues qui existent entre les coefficients d'une équation et les sommes des puissances semblables de ses racines. Il est facile de voir qu'à l'aide de ces relations on peut obtenir successivement tous les coefficients d'une équation lorsque les sommes des puissances de ses racines sont connues, comme cela arrive ici, la somme des puissances $m^{\text{ièmes}}$ des racines de l'équation :

$$H\left(x - e^{\frac{2\theta\pi i}{P}}\right) = 0$$

résultant sans difficulté de la formule (1) du paragraphe précédent.

On trouve ainsi, en supposant par exemple $P = 3 \cdot 11$:

$$Y = 2x^{10} - x^9 + 8x^8 + 5x^7 + 2x^6 + 14x^5 + 2x^4 + 5x^3 + 8x^2 - x + 2,$$

$$Z = x^9 + x^7 + 2x^6 + 2x^4 + x^3 + x,$$

par suite :

$$Y_1 = 46, \quad Z_1 = 8.$$

et comme on a $\left(\frac{2}{P}\right) = 1$:

$$\left(\frac{Y_1+Z_1\sqrt{P}}{2}\right)^{4-2\left(\frac{2}{P}\right)} = (23+4\sqrt{33})^2.$$

On a d'un autre côté:

$$T+U\sqrt{P} = 23+4\sqrt{33}.$$

d'où il suit $h = 2$, ce qui est exact, les formes qui dépendent au déterminant 33, étant $x^2 - 33y^2$, $33x^2 - y^2$.

Pour donner un exemple du cas où P se réduit à un nombre premier, soit $P = 17$: on trouve alors $Y_1 = 34$, $Z_1 = 8$, et l'expression:

$$\left(\frac{Y_1+Z_1\sqrt{P}}{2\sqrt{P}}\right)^{4-2\left(\frac{2}{P}\right)}$$

devient $(4+\sqrt{17})^2 = 33+8\sqrt{17}$, ce qui est la première puissance de $T+U\sqrt{P}$, comme cela doit être, puisque pour le déterminant 17 il n'existe que la seule forme $x^2 - 17y^2$.

Les expressions de h , relatives aux déterminants négatifs, n'ont besoin d'aucune explication. Nous ajouterons seulement que pour un cas particulier qui se rapporte au n^o. V, le résultat avait déjà été indiqué par M. JACOBI. (Voir le Journal de CRELLE Tome IX.)

Nous terminerons ce mémoire en indiquant une application que l'on peut faire des expressions de h , dans le cas des déterminants négatifs. On sait que, lorsqu'un entier k peut être décomposé en trois carrés, ou en d'autres termes lorsque l'équation $x^2+y^2+z^2 = k$ est possible, le nombre de ses solutions dépend du nombre des formes dont le déterminant est $-k$. Les théorèmes qui fixent cette dépendance, ont d'abord été découverts par LEGENDRE dans les cas les plus simples et par voie d'induction. M. GAUSS les a ensuite démontrés d'une manière générale et très ingénieuse dans la 5^{ème} section de son ouvrage. Il est évident qu'il suffit de comparer les théorèmes dont il s'agit avec les résultats auxquels nous sommes parvenus dans ce paragraphe et dans le §. 8, pour en conclure, par la simple élimination du nombre des formes quadratiques qui entre dans les uns et dans les autres, de nouvelles expressions pour le nombre des solutions de l'équation $x^2+y^2+z^2 = k$, expressions qui ne renfermeront plus rien qui soit relatif aux formes quadratiques. Je me bornerai ici à cette seule remarque et je n'entreprendrai pas quant à présent l'énumération de ces nouveaux théorèmes; ces détails seront mieux placés dans un autre mémoire dans lequel je chercherai à établir les résultats dont il s'agit d'une manière directe et sans y faire concourir les deux théories dont je viens de parler.

ÜBER EINE EIGENSCHAFT DER QUADRATISCHEN FORMEN.

VON

G. LEJEUNE DIRICHLET.

Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1840, S. 49—52.

ÜBER EINE EIGENSCHAFT DER QUADRATISCHEN FORMEN.

[Auszug aus einer in der Akademie der Wissenschaften am 5. März 1840 gelesenen Abhandlung.]

Die vorgelesene Abhandlung ist als die Fortsetzung einer früheren zu betrachten, welche in dem Jahrgange von 1837 gedruckt ist, und worin der erste strenge Beweis des Satzes gegeben worden ist, dass jede arithmetische Reihe, deren erstes Glied und deren Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält*). In der gegenwärtigen Abhandlung wird dieser Satz auf quadratische Formen, d. h. auf Ausdrücke von der Gestalt $ax^2 + 2bxy + cy^2$ angedehnt, die jedoch der Beschränkung unterworfen werden müssen, dass die darin enthaltenen bestimmten Zahlen a , $2b$, c keinen gemeinschaftlichen Factor haben.

Die Principien, auf welchen der Beweis dieser Eigenschaft beruht, obgleich im Wesentlichen mit denjenigen übereinstimmend, von welchen in der angeführten Abhandlung Gebrauch gemacht worden ist, bedürfen zum Behufe dieser neuen Anwendung einiger Modificationen, welche wir an einem speciellen Falle anzudeuten versuchen wollen. Es ist dies der Fall, wo die Determinante eine negative Primzahl $-p$ ist, welche, abgesehen vom Zeichen, die Form $4n+3$ hat, und wo diese Determinante zugleich zu den sogenannten regelmässigen gehört (*determinans regularis*, *Disq. arith. art. 306*, VI).

Es sei $h = 2\lambda + 1$ die Anzahl der verschiedenen Formen, welche für die Determinante $-p$ stattfinden, und welche unter der gemachten Voraussetzung sich alle aus einer derselben, g_1 , durch successives Zusammensetzen bilden lassen. Diese Formen, welche wir durch g bezeichnen und durch Indices von einander unterscheiden wollen, lassen sich dann immer in folgende

*) S. 313 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

Ordnung bringen:

$$(1) \quad g_{-i}, g_{-(i-1)}, \dots, g_{-1}, g_0, g_1, \dots, g_{i-1}, g_i,$$

welche Reihe als in sich zurückkehrend zu betrachten ist, so dass auf g_i wieder g_{-i} folgt, und wo jede Form aus der vorhergehenden und der Form g_1 zusammengesetzt ist. g_0 die Hauptform $x^2 + py^2$ bedeutet, und entgegengesetzten Formen:

$$ax^2 + 2bxy + cy^2, \quad ax^2 - 2bxy + cy^2.$$

entgegengesetzte Indices entsprechen.

Theilt man die Gesamtheit der positiven ungeraden Primzahlen (p ausgenommen) in zwei Classen, von welchen die erste alle diejenigen enthält, in Bezug auf welche $-p$ quadratischer Rest ist, die zweite alle übrigen umfasst, und bezeichnet die in den beiden Classen enthaltenen Zahlen allgemein respective mit f und g , so lassen sich bekanntlich die Primzahlen der ersten Classe ausschliesslich durch die Formen (1) darstellen, und zwar ist jede Primzahl f fähig, durch zwei entgegengesetzte Formen:

$$g_\gamma \quad \text{und} \quad g_{-\gamma},$$

und nur durch diese ausgedrückt zu werden: wobei es sich von selbst versteht, dass für $\gamma = 0$ diese beiden Formen sich auf die Hauptform reduciren. Der doppelte Werth:

$$\pm \gamma$$

soll nun der Index von f heissen.

Es sei ferner:

$$\frac{2\pi}{h} = \omega,$$

wo π die gewöhnliche Bedeutung hat, t irgend eine der Zahlen:

$$(2) \quad 0, 1, 2, \dots, \lambda$$

und endlich s eine positive die Einheit übertreffende Grösse. Alsdann findet folgende Gleichung statt, deren Wahrheit leicht aus den bekannten Sätzen über die Zusammensetzung der Formen folgt:

$$2H \frac{1}{1 - \frac{1}{f^{2s}}} \cdot H \frac{1}{1 - 2 \frac{\cos \gamma \omega}{f^s} + \frac{1}{f^{2s}}} = \Sigma \frac{1}{g_0^s} + 2 \cos \omega \Sigma \frac{1}{g_1^s} + \dots + 2 \cos \lambda t \omega \Sigma \frac{1}{g_\lambda^s}.$$

In dieser Gleichung bezieht sich das erste Multiplicationszeichen auf alle Primzahlen g , das zweite auf alle Primzahlen f , und $\pm \gamma$ ist der jedesmalige Index

von f . Was das Zeichen Σ betrifft, so bedeutet dasselbe, dass man in der quadratischen Form, vor welcher es steht, den unbestimmten Zahlen x und y alle Systeme positiver oder negativer Werthe von solcher Beschaffenheit beilegen muss, dass der entsprechende Werth der Form ungerade und nicht durch p theilbar wird. Setzt man zur Abkürzung:

$$2H \frac{1}{1 - \frac{1}{g^{2s}}} = G$$

und bezeichnet die rechte Seite der Gleichung mit L , nimmt dann die Logarithmen von beiden Seiten und entwickelt jeden der Logarithmen, welche f enthalten, nach der bekannten Formel:

$$-\frac{1}{2} \log(1 - 2z \cos \alpha + z^2) = \frac{z}{1} \cos \alpha + \frac{z^2}{2} \cos 2\alpha + \dots,$$

so erhält man:

$$\Sigma \frac{\cos t \gamma \omega}{f^s} + \frac{1}{2} \Sigma \frac{\cos 2t \gamma \omega}{f^{2s}} + \dots = -\frac{1}{2} \log G + \frac{1}{2} \log L.$$

Diese allgemeine Gleichung enthält, wie die frühere, $\lambda + 1$ besondere Gleichungen, welche den verschiedenen Werthen (2) von t entsprechen. Addirt man diese besonderen Gleichungen, nachdem man sie der Reihe nach mit:

$$1, 2 \cos \mu \omega, 2 \cos 2 \mu \omega, \dots, 2 \cos \lambda \mu \omega$$

multipliziert hat, und nimmt man für μ eine der Zahlen $1, 2, \dots, \lambda$, so kommt:

$$(3) \quad \Sigma \frac{1}{f^s} + \frac{1}{2} \Sigma \frac{1}{f^{2s}} + \dots = \frac{1}{h} (\log L_0 + 2 \cos \mu \omega \log L_1 + \dots + 2 \cos \lambda \mu \omega \log L_\lambda),$$

wobei die erste Summation auf alle Primzahlen auszudehnen ist, deren Index $\pm \mu$ ist, die zweite auf diejenigen, deren doppelt genommener Index congruent $\pm \mu$ (mod. h) ist, u. s. w. Für $\mu = 0$ erhält man durch dasselbe Verfahren:

$$(4) \quad \Sigma \frac{1}{f^s} + \frac{1}{2} \Sigma \frac{1}{f^{2s}} + \dots = -\frac{1}{2} \log G + \frac{1}{2h} (\log L_0 + 2 \log L_1 + \dots + 2 \log L_\lambda),$$

wobei die Summation sich resp. über alle Primzahlen erstreckt, deren Indices, resp. mit $1, 2, \dots$ multipliziert, durch h theilbar werden.

Die Gleichungen (3) und (4) gelten, wie diejenigen, aus welchen sie abgeleitet sind, für jeden Werth von s , welcher grösser als 1 ist. Setzt man daher:

$$s = 1 + \epsilon,$$

wo ϱ positiv angenommen ist, so kann man die Veränderliche ϱ unendlich klein werden lassen. Untersucht man nun die unter dem Logarithmenzeichen vorkommenden Ausdrücke in dieser Voraussetzung, so findet man durch sehr einfache Betrachtungen, die jedoch hier nicht ausgeführt werden können, dass L_0 unendlich wird, dass hingegen L_t , wenn t nicht den Werth 0 hat, sich einer endlichen, von der Null verschiedenen Grenze nähert, und dass dieselbe Eigenschaft dem Producte G zukommt. Aus diesem Resultate folgt sogleich, dass die zweite und also auch die erste Seite jeder von den Gleichungen (3) und (4) für ein unendlich kleines ϱ unendlich gross wird, und dann ferner, wie in der früheren Abhandlung, dass die Summe:

$$\sum \frac{1}{j^{1+\varrho}}$$

aus unendlich vielen Gliedern besteht, oder, was dasselbe ist, dass jede der Formen (1) eine unendliche Anzahl von Primzahlen enthält.

UNTERSUCHUNGEN
ÜBER DIE THEORIE DER COMPLEXEN ZAHLEN.

VON

G. LEJEUNE DIRICHLET.

Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1841, S. 190—194.

UNTERSUCHUNGEN ÜBER DIE THEORIE DER COMPLEXEN ZAHLEN.

[Auszug aus einer in der Akademie der Wissenschaften am 27. Mai 1841 gelesenen Abhandlung.]

Da sich diese Untersuchungen, sowohl hinsichtlich der darin befolgten Methode als durch ihre Resultate, an frühere Arbeiten des Verfassers anschliessen, so wird es zur leichteren Verständlichkeit der hier zu gebenden Andeutungen zweckmässig sein, wenn wir diesen eine kurze Erwähnung einiger der früher behandelten Fragen vorausschicken.

In einer Abhandlung, welche unter denen der Akademie für das Jahr 1837 gedruckt ist^{*)}, hat man sich die Aufgabe gestellt, den längst bekannten und oft als Lemma benutzten Satz, nach welchem jede arithmetische Reihe, deren erstes Glied und deren Differenz keinen gemeinschaftlichen Factor haben, eine unendliche Anzahl von Primzahlen enthält, in aller Strenge zu beweisen. Der dort entwickelte Beweis bietet das Merkwürdige dar, dass er ungeachtet der rein arithmetischen Natur des zu begründenden Satzes wesentlich auf der Betrachtung stetig veränderlicher Grössen beruht, indem derselbe von der Bildung unendlicher Reihen ausgeht, die wie die schon von EULER in der *Introd. in Anal. inf.* behandelten durch Multiplication einer unendlichen Anzahl von Factoren entstehen. Diese neuen Reihen unterscheiden sich jedoch darin von den EULER'schen, dass in die Factoren, von denen jeder ein Glied der Reihe der Primzahlen enthält, noch Potenzen von Wurzeln der Einheit eingehen, deren Exponenten mit den sogenannten Indices der Primzahlen zusammenfallen, wenn diese mit allen übrigen auf ein System primitiver Wurzeln bezogen wird. Sobald man den eben angedeuteten Weg betreten hat, scheint sich der Beweis mit der grössten Leichtigkeit

^{*)} S. 313 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.
G. Lejeune Dirichlet's Werke.

und, so zu sagen, ganz von selbst zu gestalten; allein bei aufmerksamer Betrachtung bemerkt man eine Schwierigkeit, ohne deren Beseitigung das Verfahren ganz illusorisch werden oder doch nur auf besondere Fälle anwendbar sein würde. Diese Schwierigkeit besteht in der für den Erfolg unerlässlichen Nachweisung, dass die Summen gewisser Reihen, deren Convergenz leicht einzusehen ist, von der Null verschieden sind, und hat nicht etwa, wie man es zunächst vermuthen sollte, ihren Grund in der Unmöglichkeit die Summation auszuführen. Diese Operation ist vielmehr in allen Fällen leicht zu bewerkstelligen; allein der endliche Ausdruck, welchen man dadurch erhält, gewährt keine Erleichterung für die geforderte Nachweisung, und es ist im Allgemeinen eben so schwer aus der Summe in endlicher Form zu erkennen, dass sie von Null verschieden ist, als dies bei der ursprünglichen Reihe der Fall war.

Nach mancherlei fruchtlosen Versuchen war es zwar gelungen, die erwähnte Schwierigkeit vollständig zu überwinden; doch waren die Betrachtungen, zu welchen man seine Zuflucht zu nehmen genöthigt war, so complicirt und indirect, dass sie nur wenig befriedigen konnten und die Auffindung eines kürzeren und der Natur der Sache mehr entsprechenden Verfahrens sehr wünschenswerth machen mussten. Wiederholte auf diesen Gegenstand gerichtete Bemühungen hatten denn auch endlich den beabsichtigten Erfolg und führten zu dem unerwarteten Resultate, dass die erwähnten Reihen mit einer Aufgabe zusammenhängen, deren Lösung in einem der wichtigsten Theile der Zahlenlehre eine längst gefühlte Lücke ausfüllt. Die Theorie, von welcher wir reden, ist die der quadratischen Formen, welche zuerst von LAGRANGE begründet, später durch LEGENDRE und besonders durch GAUSS zu einem hohen Grade der Ausbildung gelangt ist. Bekanntlich sind die Eigenschaften solcher Formen hauptsächlich von einer durch ihre Coefficienten bestimmten ganzen Zahl, welche die Determinante der Form heisst, abhängig, und LAGRANGE hat gezeigt, dass jeder Determinante, sie sei positiv oder negativ, nur eine endliche Anzahl wesentlich verschiedener Formen entspricht, so wie derselbe grosse Geometer auch das Verfahren angegeben hat, nach welchem sich für jede numerisch gegebene Determinante diese wesentlich verschiedenen Formen darstellen lassen. Die Frage nach dem allgemeinen Zusammenhange zwischen der Anzahl der Formen und der Determinante wird jedoch durch die Kenntniss dieses nur in bestimmten Fällen auszuführenden Verfahrens nicht erledigt, und diese Frage ist es nun, welche in den oben erwähnten Untersuchungen ihre Lösung erhält.

Von den daraus hervorgehenden Resultaten, welche im CRELLE'schen Journal (Bd. XIX u. XXI*) ausführlich entwickelt worden sind, ist für unseren Zweck nur zu erwähnen, dass die Abhängigkeit der Anzahl der Formen von der Determinante sich in einer ganz verschiedenen Weise darstellt, je nachdem die Determinante negativ oder positiv ist. Im ersteren Falle ist diese Abhängigkeit rein arithmetischer Natur, während der Ausdruck für die Anzahl der Formen im zweiten Falle gewisse Verbindungen der Coefficienten der Hilfspgleichungen enthält, welche bei der Kreistheilung vorkommen.

Was nun die neuen Untersuchungen betrifft, deren ersten Theil die der Akademie vorgelegte Abhandlung enthält, so haben diese den Zweck, die eben angeführten Resultate auf die Theorie der complexen Zahlen auszudehnen. Den Gedanken, complexe ganze Zahlen, d. h. Ausdrücke von der Form $t+u\sqrt{-1}$, in die höhere Arithmetik einzuführen, verdankt man dem berühmten Verfasser der *Disq. arithm.*, welcher auf diese Erweiterung durch seine Untersuchungen über die Theorie der biquadratischen Reste geführt worden ist, deren Fundamentaltheoreme nur dann in ihrer höchsten Einfachheit und ganzen Schönheit erscheinen, wenn man sie auf complexe Primzahlen bezieht. Die Wichtigkeit des so erweiterten Begriffs der ganzen Zahl ist jedoch nicht auf die eben erwähnte Anwendung beschränkt: es wird vielmehr durch dessen Einführung den Untersuchungen der höheren Arithmetik ein neues Gebiet aufgeschlossen, auf welchem fast jede Eigenschaft reeller Zahlen ihr Analogon findet, welches nicht selten der ersteren hinsichtlich der Einfachheit und Eleganz gleichkommt oder sie gar übertrifft. So gilt z. B. der angeführte Satz über die arithmetische Reihe auch noch für complexe Zahlen, d. h. der Ausdruck $an+b$ enthält unendlich viele complexe Primzahlen, wenn man darin a und b als gegebene complexe Zahlen ohne gemeinschaftlichen Factor, n dagegen als eine unbestimmte complexe Zahl betrachtet. Der Beweis bleibt dem für reelle Zahlen sehr ähnlich, und diese Ähnlichkeit erstreckt sich auch auf den hier gleichfalls vorkommenden Umstand, dass man zu zeigen hat, dass gewisse convergirende Reihen Summen haben, welche von Null verschieden sind. Die Analogie machte es im höchsten Grade wahrscheinlich, dass zwischen diesen Reihen und der Anzahl der quadratischen Formen für die entsprechende complexe Determinante ein ähnlicher Zusammenhang stattfinden müsse, wie er früher für reelle Determinanten nachgewiesen worden war.

*) S. 411 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

Doch war dieser Zusammenhang in der Theorie der complexen Zahlen weit schwerer aufzufinden, nicht nur wegen der grösseren Complication des Gegenstandes, sondern hauptsächlich deshalb, weil die Theorie der quadratischen Formen auf dem Gebiete der complexen Zahlen noch ganz unausgebildet war und es also erforderlich wurde, die bekannten Sätze der Theorie der quadratischen Formen, im gewöhnlichen Sinne des Wortes, der Reihe nach durchzugehen, um zu erkennen, mit welchen Modificationen sie für complexe Zahlen gelten.

Nach dieser vorläufigen Untersuchung gelangt man in der That dahin, den vermutheten Zusammenhang nachzuweisen, und es bleibt alsdann nur noch übrig, die erwähnten Reihen zu summiren, um den Ausdruck zu erhalten, welcher die Anzahl der Formen für eine complexe Determinante als Function dieser Determinante bestimmt. Als schliessliches Resultat der Untersuchung stellt sich heraus, dass die Abhängigkeit der Anzahl der Formen von der Determinante derjenigen ganz ähnlich ist, welche in dem zweiten der oben angeführten Fälle stattfindet, nur mit dem Unterschiede, dass die Rolle, welche dort die Hilfspgleichungen für die Kreistheilung spielen, hier von den Gleichungen übernommen wird, welche sich auf die Theilung der Lemniscate oder, was dasselbe ist, auf die Theilung der elliptischen Functionen beziehen, welche dem Modul $\sqrt{\frac{1}{2}}$ entsprechen.

Merkwürdiger noch als dieses allgemeine Resultat ist ein besonderer Fall, wo die Anzahl der Formen unabhängig von der Theilung der Lemniscate bestimmt werden kann. Es ist dies der Fall einer reellen Determinante D ; für eine solche ist nämlich, wenn man sie in der Theorie der complexen Zahlen betrachtet, die Anzahl der Formen ein Product von drei Factoren, von welchen der erste eine einfache algebraische Function der Determinante darstellt, während der zweite und dritte mit den Zahlen zusammenfallen, welche in der gewöhnlichen Theorie der quadratischen Formen bezeichnen, wie viel Formen für die Determinanten $+D$ und $-D$ stattfinden. Dieses Resultat enthält, wenn wir uns nicht sehr täuschen, einen der schönsten Sätze der Theorie der complexen Zahlen und muss um so mehr überraschen, als in der Theorie der reellen Zahlen zwischen den Formen, welche zwei entgegengesetzten Determinanten entsprechen, gar kein Zusammenhang zu bestehen scheint.

UNTERSUCHUNGEN
ÜBER DIE THEORIE DER COMPLEXEN ZAHLEN.

VON

G. LEJEUNE DIRICHLET.

Abhandlungen der Königlich Preussischen Akademie der Wissenschaften von 1841, S. 141 — 161.

UNTERSUCHUNGEN ÜBER DIE THEORIE DER COMPLEXEN ZAHLEN.

[Gelesen in der Akademie der Wissenschaften am 27. Mai 1841.]

Gegenwärtige Abhandlung bildet einen Theil einer grösseren Arbeit, welche den Zweck hat, mehrere der Theorie der reellen ganzen Zahlen angehörige, früher von mir gelöste Fragen auf das Gebiet der complexen Zahlen zu verpflanzen und vermittelst derselben Methode, von welcher in den erwähnten Untersuchungen Gebrauch gemacht worden ist, zu behandeln. Zu dieser Erweiterung hat mich nicht nur die Aussicht auf die neuen Resultate, welche sich von derselben erwarten liessen, sondern auch und mehr noch der Wunsch bestimmt, auf solche Weise jene frühere Behandlungsweise einer Prüfung zu unterwerfen und klar zu übersehen, ob der Erfolg derselben einer wirklichen Übereinstimmung der Methode mit der wahren Natur der gelösten Fragen oder, wie es bei mathematischen Untersuchungen nicht selten der Fall ist, mehr zufälligen Umständen zuzuschreiben sei. Diese Probe nun hat die Methode mit Glück bestanden, indem es nur geringer, sich ganz von selbst aus der veränderten Beschaffenheit des Gegenstandes ergebender Modificationen bedurfte, um sie auf die analogen, der Theorie der complexen Zahlen angehörigen Fragen anwendbar zu machen.

Der bei weitem grössere Theil der neuen Untersuchungen, deren Zweck ich im Vorhergehenden bezeichnet habe, bezieht sich auf die Lehre von den quadratischen Formen und wird nächstens an einem anderen Orte erscheinen.*) In der gegenwärtigen Abhandlung beschäftige ich mich ausschliesslich mit dem Beweise des Satzes, dass der Ausdruck $kt+l$, in welchem l eine unbestimmte complexe ganze Zahl und k, l gegebene solche Zahlen ohne gemeinschaftlichen Factor bezeichnen, immer unendlich viele Primzahlen enthält. Dieser Beweis

*) S. 333 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

setzt, wie der früher gegebene des analogen Satzes für reelle Zahlen, ausser den Fundamentalsätzen über die complexen Zahlen gewisse Eigenschaften der quadratischen Formen voraus, weshalb ich mich, um unnütze Wiederholungen zu vermeiden, auf die eben erwähnten Untersuchungen berufen werde*).

§. 1.

Ogleich, wie schon bemerkt worden, die Elementareigenschaften der complexen Zahlen als bekannt vorausgesetzt werden, so wird es doch zweckmässig sein, einige dieser Eigenschaften, welche für das Folgende von besonderer Wichtigkeit sind, hier ganz kurz anzugeben.

Wir setzen, wie gewöhnlich, $\sqrt{-1} = i$ und nennen complexe ganze Zahl jeden Ausdruck $f+gi$, in welchem f und g reelle ganze Zahlen bedeuten. Die der complexen Zahl $f+gi$ entsprechende positive Zahl f^2+g^2 wird ihre Norm genannt und mit $N(f+gi)$ bezeichnet werden. Vier complexe Zahlen:

$$f+gi, \quad -g+fi, \quad -f-gi, \quad g-fi,$$

welche so von einander abhängen, dass irgend drei derselben aus der vierten entstehen, wenn man diese mit -1 , $\pm i$ multiplicirt, sollen *zusammengehörig* heissen.

In Bezug auf einen gegebenen complexen Modul m lässt sich immer eine Zahlenreihe bilden, welche die doppelte Eigenschaft besitzt, dass sich unter ihren Gliedern eines und nur eines befindet, welches mit einer beliebigen Zahl nach dem Modul m congruent ist.

Die Anzahl der Glieder eines solchen Systems incongruenter Zahlen ist $N(m)$. Auch lässt sich allgemein bestimmen, wie viel Glieder es in einem solchen Systeme giebt, die mit m keinen gemeinschaftlichen Factor haben.

Setzt man nämlich:

$$(1) \quad m = i^a a^b b^c c^d \dots,$$

wo a, b, c, \dots Primzahlen bedeuten, von denen keine der anderen gleich ist

*) Diese Untersuchungen sind, seit gegenwärtige Abhandlung der Akademie vorgelegt worden ist, unter dem Titel „Recherches sur les formes quadratiques à coefficients et à indéterminées complexes“ im CRELLESchen Journal Band XXIV bekannt gemacht worden.†) Ausser dem im Titel angegebenen Gegenstande enthält die eben angeführte Abhandlung eine kurze Darstellung der Elemente der Theorie der complexen Zahlen, wobei ich mich jedoch auf die Sätze beschränkt habe, die zum Verständniss jener Abhandlung erforderlich waren. Eine vollständigere Darstellung dieser Elemente findet man in der zweiten Abhandlung über die biquadratischen Reste von GAUSS, in welcher dieser grosse Geometer den Begriff der complexen Zahl zuerst in die Wissenschaft eingeführt hat, und auf welche ich den Leser verweise.

†) S. 333 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

noch mit ihr zusammengehört, und setzt ferner:

$$N(a) = A, \quad N(b) = B, \quad N(c) = C, \quad \dots,$$

so wird die verlangte Anzahl $\psi(m)$ durch die Gleichung:

$$\psi(m) = (A-1)A^{a-1} \cdot (B-1)B^{b-1} \cdot (C-1)C^{c-1} \dots$$

gegeben.

Sind:

$$(2) \quad \mu, \mu', \mu'', \dots$$

die Glieder, deren Anzahl so eben bestimmt wurde, und bezeichnet l eine Zahl, die mit m keinen gemeinschaftlichen Factor hat, so beweist man leicht, dass die Zahlen:

$$l\mu, l\mu', l\mu'', \dots$$

wenn man von ihrer Ordnung absieht, mit den Zahlen (2) nach dem Modul m congruent sind, und hieraus erschliesst man, wie in dem bekannten Beweise des FERMAT'schen Satzes für reelle Zahlen, die Congruenz:

$$(3) \quad l^{\psi(m)} \equiv 1 \pmod{m}.$$

Wie man in der gewöhnlichen Zahlentheorie die positiven Zahlen als die ursprünglichen und die negativen als durch Multiplication mit dem Factor -1 aus diesen entstanden zu betrachten pflegt, so gewährt es für manche auf complexe Zahlen bezügliche Betrachtungen eine wesentliche Erleichterung, wenn man unter je vier zusammengehörigen Zahlen eine nach einem festen Princip gewählte als die ursprüngliche oder primäre und die übrigen als die Producte dieser in $-1, \pm i$ ansieht. Das Bedürfniss einer solchen Unterscheidung ist besonders bei der Betrachtung ungerader Zahlen fühlbar, und man hat bei der zu treffenden Wahl darauf zu sehen, dass, wie das Product von positiven Factoren selbst wieder positiv ist, so auch hier aus der Multiplication primärer Factoren wieder eine primäre Zahl hervorgehe. Wie leicht zu sehen, findet sich in jeder Gruppe zusammengehöriger ungerader Zahlen immer eine und nur eine Zahl $f+gi$, für welche f und g resp. die Form $4\mu+1$ und 2μ haben, so wie auch nur eine, für welche $f-1$ und g entweder beide in der Form 4μ oder beide in der Form $4\mu+2$ enthalten sind, und man überzeugt sich ohne Schwierigkeit, dass der eben ausgesprochenen Bedingung Genüge geschieht, welche dieser Zahlen man auch allgemein, d. h. für alle Gruppen zusammengehöriger Zahlen, als die primäre betrachte. In der oben citirten Abhandlung haben wir die erste Definition gewählt; doch bleibt alles dort Gesagte wörtlich

richtig, wenn die zweite Definition zu Grunde gelegt wird. Diese letztere ist für unseren gegenwärtigen Zweck vorzuziehen: wir werden deshalb in dieser Abhandlung diejenigen ungeraden Zahlen $f+gi$ als primär betrachten, für welche $f-1$ und g gleichzeitig die Form 4μ oder gleichzeitig die Form $4\mu+2$ haben, und bemerken nur noch zur leichteren Anwendung dieser Definition, dass dieselbe offenbar darauf hinauskommt, in jeder Gruppe zusammengehöriger ungerader Zahlen diejenige als primär zu bezeichnen, welche nach dem Modul $2+2i$ der positiven Einheit congruent ist.

Unter dieser Voraussetzung hat man für jede ungerade primäre Zahl m :

$$(4) \quad m = a^{\alpha} b^{\beta} c^{\gamma} \dots,$$

won a, b, c, \dots von einander verschiedene primäre Primzahlen bedeuten, welche so wie ihre Exponenten durch m vollständig bestimmt sind.

§. 2.

Ehe wir an die Behandlung der Frage gehen können, welche den eigentlichen Gegenstand dieser Abhandlung bildet, sind einige Eigenschaften der Potenzreste für complexe Moduln abzuleiten.

Sind k und l zwei complexe Zahlen ohne gemeinschaftlichen Factor, und ist e der kleinste von Null verschiedene Exponent, für den $l^e \equiv 1 \pmod{k}$ ist, so sagt man, l gehöre für den Modul k zum Exponenten e . Es ist leicht sich zu überzeugen, dass alsdann:

$$1, l, l^2, \dots, l^{e-1}$$

nach dem Modul k incongruent sind, so wie auch dass, wenn man die Reihe weiter fortsetzt, dieselben Reste periodisch wiederkehren, so dass also nur diejenigen Potenzen, deren Exponenten Vielfache von e sind, der Einheit congruent werden. Da:

$$l^{\psi(k)} \equiv 1 \pmod{k}$$

ist, so wird also e immer ein Theiler von $\psi(k)$ sein. In dem speciellen Falle, wo $e = \psi(k)$ ist, bilden die Potenzen:

$$1, l, l^2, \dots, l^{\psi(k)-1}$$

ein System, wie wir es im vorigen Paragraphen betrachtet haben, d. h. welches ein Glied, aber auch nur eines enthält, welches mit einer beliebigen Zahl, die mit k keinen gemeinschaftlichen Factor hat, nach dem Modul k congruent

ist, und l heisst dann eine primitive Wurzel von k . Kennt man den Exponenten e , zu welchem l gehört, so kann man leicht denjenigen bestimmen, zu dem irgend eine Potenz l^s von l gehört. Man sieht ohne Schwierigkeit, dass dieser Exponent gleich $\frac{e}{\delta}$ ist, wenn δ den grössten gemeinschaftlichen (positiven) Theiler von s und e bezeichnet.

I. Wir betrachten zuerst den Fall, wo der Modul eine Potenz $(a+bi)^f$ einer ungeraden zweigliedrigen Primzahl $a+bi$ ist, so dass also:

$$N(a+bi) = a^2 + b^2 = p$$

eine reelle Primzahl $4\mu+1$ ist. Für diesen Fall ist es leicht, die Existenz einer primitiven Wurzel zu zeigen. Ist die reelle Zahl a eine primitive Wurzel für den Modul p^f , so wird sie es auch in Bezug auf den Modul $(a+bi)^f$ sein. Da nämlich nach der ausgesprochenen Voraussetzung:

$$1, a, a^2, \dots, a^{(p-1)p^{f-1}}$$

nach dem Modul p^f incongruent sind, so haben sie dieselbe Eigenschaft für den Modul $(a+bi)^f$, und andererseits ist:

$$\psi((a+bi)^f) = (p-1)p^{f-1}.$$

Hat man eine solche primitive Wurzel a gewählt, so soll der Exponent:

$$\alpha_n < (p-1)p^{f-1},$$

für welchen:

$$\alpha_n \equiv n \pmod{(a+bi)^f}$$

ist, der Index der beliebigen nicht durch $a+bi$ theilbaren Zahl n heissen. Es folgt unmittelbar aus dieser Definition, dass man den Index eines Productes erhält, wenn man von der Summe der Indices der Factoren das grösste darin enthaltene Vielfache von $(p-1)p^{f-1}$ abzieht.

Die Zahl a ist immer quadratischer Nichtrest von $a+bi$, da sonst jedes n quadratischer Rest von $a+bi$ sein müsste. Hieraus folgt sogleich, dass α_n gerade oder ungerade sein wird, je nachdem n quadratischer Rest oder Nichtrest von $a+bi$ ist. Man hat daher, wenn man sich des in der oben citirten Abhandlung eingeführten Zeichens bedient:

$$(5) \quad \left[\frac{n}{a+bi} \right] = (-1)^{\alpha_n}.$$

II. Der jetzt zu behandelnde Fall ist der eines Moduls von der Form r^g , wo r eine eingliedrige Primzahl bezeichnet. Da wir r reell und positiv voraussetzen können, so ist r eine Primzahl $4\mu + 3$.

Zu dieser Untersuchung ist die Congruenz:

$$(b+zc)^{r^{g-2}} \equiv b^{r^{g-2}} + ezb^{r^{g-2}-1}r^{g-1} \pmod{r^g}$$

erforderlich, welche schon in den *Disq. arith.* (art. 86) benutzt worden ist. Es ist zwar dort angenommen worden, dass b und z reell sind, aber derselbe Beweis ist auch auf den Fall anwendbar, wo b und z complexe Zahlen sind. Die im Exponenten vorkommenden Zahlen e und $g \geq 2$ sind, wie sich von selbst versteht, positiv.

Für den Modul r^g existirt keine primitive Wurzel, ausser wenn $g = 1$ ist: denn es ist mit Hülfe der obigen Congruenz leicht einzusehen, dass der höchste Exponent, zu welchem eine Zahl für diesen Modul gehören kann, $(r^2-1)r^{g-1}$ ist, während:

$$\psi(r^g) = (r^2-1)r^{2g-2}$$

ist. Dass es aber zum Exponenten $(r^2-1)r^{g-1}$ gehörende Zahlen giebt, kann man, wie folgt, zeigen. Da die aufgestellte Behauptung für $g = 1$ schon erwiesen ist (*Theor. res. biq. auct.* C. F. GAUSS art. 53), so sei b eine für den Modul r zum Exponenten r^2-1 gehörige Zahl, d. h. eine primitive Wurzel von r . Unter dieser Voraussetzung wird:

$$(b+zc)^e - 1$$

nur dann durch r theilbar sein, wenn e ein Vielfaches von r^2-1 ist. Es folgt hieraus, dass der Exponent, zu dem $b+zc$ für den Modul r^g gehört, durch r^2-1 theilbar sein muss. Da aber andererseits auch:

$$(b+zc)^{(r^2-1)r^{g-1}} \equiv 1 \pmod{r^g}$$

ist, wie aus obiger Congruenz sogleich folgt, wenn man:

$$(b+zc)^{r^2-1} = 1 + ur$$

setzt, so sieht man, dass der erwähnte Exponent ein Theiler von $(r^2-1)r^{g-1}$ sein muss. Man wird daher eine zum Exponenten $(r^2-1)r^{g-1}$ gehörige Zahl $b+zc$ finden können, wenn sich z so wählen lässt, dass nicht:

$$(b+zc)^{(r^2-1)r^{g-2}} \equiv 1 \pmod{r^g}$$

ist. Es ist aber nach obigem Lemma:

$$-1 + (b+zc)^{(r^2-1)r^{g-2}} \equiv -1 + b^{(r^2-1)r^{g-2}} + (r^2-1)zb^{(r^2-1)r^{g-2}-1}r^{g-1} \pmod{r^g},$$

Berücksichtigt man nun, dass:

$$-1 + b^{(r^2-1)r^{g-2}} = B r^{g-1}$$

ist, wo B eine ganze Zahl bedeutet, und setzt zur Abkürzung:

$$(r^2-1)b^{(r^2-1)r^{g-2}-1} = C,$$

so ist klar, dass die geforderte Bedingung erfüllt sein wird, sobald man z so wählt, dass die Congruenz $Cz + B \equiv 0 \pmod{r}$ nicht stattfindet: und dies kann immer geschehen, da C kein Vielfaches von r ist.

Es liesse sich das eben erhaltene Resultat leicht vervollständigen und allgemein bestimmen, wie viel verschiedene, d. h. incongruente Zahlen zum Exponenten $(r^2-1)r^{g-1}$ oder überhaupt zu irgend einem Divisor desselben gehören. Ist $e r^\nu$ ein solcher, wo e in r^2-1 aufgeht, und $\nu \geq g-1$, so wird die fragliche Anzahl durch den Ausdruck $g(e)\psi(r^\nu)$ gegeben, worin $g(e)$ die Anzahl der Zahlen bezeichnet, welche in der Reihe $0, 1, 2, \dots, e-1$ keinen gemeinschaftlichen Factor mit e haben. Da aber die Kenntniss dieser Anzahl zu unserem Zwecke nicht erforderlich ist, so wollen wir uns bei deren Bestimmung nicht aufhalten. Das Einzige, was für das Folgende nöthig ist, betrifft die Form der zum Exponenten r^{g-1} gehörigen Zahlen, welche sehr leicht auszumitteln ist. Wenn c zu dem genannten Exponenten gehört, so dass also $c r^{g-1} - 1$ durch r^g und folglich auch durch r theilbar ist, so wird r^{g-1} ein Vielfaches von dem Exponenten sein, zu dem c für den Modul r gehört. Da der letztere Exponent aber auch andererseits ein Theiler von r^2-1 sein muss, so hat derselbe den Werth 1, d. h. c ist von der Form $1+zr$, und es bleibt nur noch zu untersuchen, welcher Bedingung z unterworfen sein muss, damit $1+zr$ für den Modul r^g wirklich zum Exponenten r^{g-1} gehöre. Zu diesem Zwecke bemerke man, dass, da nach dem obigen Lemma:

$$(1+zr)^{r^{g-1}} - 1$$

offenbar durch r^g theilbar ist, der Exponent, zu dem $1+zr$ gehört, in r^{g-1} aufgehen und also kein anderer als r^{g-1} selbst sein wird, wenn z so beschaffen ist, dass die Congruenz:

$$(1+zr)^{r^{g-2}} \equiv 1 \pmod{r^g}$$

nicht stattfindet. Giebt man dieser mit Hülfe des Lemmas die Form:

$$z r^{g-1} \equiv 0 \pmod{r^g},$$

so sieht man, dass die nöthige und ausreichende Bedingung, damit c zum Ex-

ponenten r^{g-1} gehöre, darin besteht, dass ϵ in dem Ausdruck $1+zr$ enthalten und z kein Vielfaches von r sei.

Dies vorausgesetzt, wird es uns leicht sein nachzuweisen, dass, wenn \mathfrak{b} eine gegebene zum Exponenten $(r^2-1)r^{g-1}$ gehörige Zahl ist, immer eine zweite zum Exponenten r^{g-1} gehörige Zahl $\epsilon = 1+zr$ von solcher Beschaffenheit gefunden werden kann, dass die Congruenz:

$$\mathfrak{b}^{\beta} \equiv \epsilon^{\gamma} \pmod{r^g},$$

worin β und γ resp. in den Reihen:

$$0, 1, 2, \dots, (r^2-1)r^{g-1}-1; 0, 1, \dots, r^{g-1}-1$$

enthaltene Zahlen bedeuten, nicht anders bestehen kann, als wenn man gleichzeitig $\beta = 0$, $\gamma = 0$ hat. Wir bemerken zunächst, dass, da offenbar von den beiden Gleichungen $\beta = 0$, $\gamma = 0$ die eine die andere zur Folge hat, wir nur zu zeigen haben, dass ϵ so gewählt werden kann, dass die Congruenz nicht bestehen kann, wenn β und γ beide von Null verschieden sind. Es ist ferner leicht einzusehen, dass die Möglichkeit der Congruenz die Theilbarkeit von β durch r^2-1 voraussetzt. Setzen wir daher:

$$\beta = (r^2-1)\beta', \quad \mathfrak{b}^{r^2-1} = 1+kr,$$

wo k eine gegebene, nicht durch r theilbare Zahl bedeutet, so wird unsere Congruenz:

$$(1+kr)^{\beta'} \equiv (1+zr)^{\gamma} \pmod{r^g},$$

und es ist nur noch übrig z so einzurichten, dass dieselbe nicht bestehen kann, wenn β' und γ beide in der Reihe $1, 2, \dots, r^{g-1}-1$ gewählt werden. Da $1+kr$ und $1+zr$ zum Exponenten r^{g-1} und folglich $(1+kr)^{\beta'}$ und $(1+zr)^{\gamma}$ zu den Exponenten $r^{g-1-\lambda}$ und $r^{g-1-\mu}$ gehören, wo r^{λ} und r^{μ} die höchsten in β' und γ aufgehenden Potenzen von r bedeuten, so erfordert unsere Congruenz, dass man $\lambda = \mu$ habe, und wird, wenn man $\beta' = r^{\lambda}\beta''$ und $\gamma = r^{\lambda}\gamma'$ setzt:

$$(1+kr)^{\beta''r^{\lambda}} \equiv (1+zr)^{\gamma'r^{\lambda}} \pmod{r^g}.$$

Da $\lambda \leq g-2$ ist, und diese letztere Congruenz, für $\lambda < g-2$ als richtig vorausgesetzt, auch noch für $\lambda = g-2$ bestehen wird, so haben wir bloss zu zeigen, dass für ein gehörig gewähltes z die Congruenz:

$$(1+kr)^{\beta''r^{g-2}} \equiv (1+zr)^{\gamma'r^{g-2}} \pmod{r^g}$$

nicht stattfinden kann. Nach dem obigen Lemma ist diese ganz gleichbedeu-

tend mit:

$$(\gamma'z - \beta''k)^{r^{g-1}} \equiv 0 \pmod{r^g},$$

oder was dasselbe ist, mit:

$$\gamma'z \equiv \beta''k \pmod{r}.$$

Jetzt bemerke man, dass, da die nicht durch r theilbaren Zahlen γ' und β'' reell sind, man immer eine reelle und offenbar nicht durch r theilbare Zahl δ so bestimmen kann, dass $\beta'' \equiv \gamma'\delta \pmod{r}$ wird, wodurch die letzte Congruenz in:

$$z \equiv k\delta \pmod{r}$$

übergeht. Da δ und also auch $k\delta$ nur $r-1$ nach dem Modul r incongruente Werthe annehmen kann, während für z , welches nur die Bedingung zu erfüllen hat, nicht durch r theilbar zu sein, r^g-1 verschiedene Werthe gewählt werden können, so sieht man, dass es $r^g-1-(r-1) = r(r-1)$ incongruente Werthe von z von solcher Beschaffenheit giebt, dass die letzte Congruenz unmöglich wird, w. z. b. w.

Das eben erhaltene Resultat, nach welchem für die auf die angegebene Weise bestimmten und zu den Exponenten $(r^2-1)^{r^{g-1}}$ und r^{g-1} gehörigen Basen \mathfrak{b} und \mathfrak{c} die Congruenz:

$$\mathfrak{b}^{\mathfrak{s}} \equiv \mathfrak{c}^{\mathfrak{r}} \pmod{r^g},$$

in welcher β und γ resp. Glieder der Reihen:

$$0, 1, 2, \dots, (r^2-1)^{r^{g-1}}-1; \quad 0, 1, 2, \dots, r^{g-1}-1$$

bedeuten, nur für den Fall $\beta = \gamma = 0$ bestehen kann, lässt sich auf eine etwas verschiedene Weise aussprechen, und man überzeugt sich ohne Schwierigkeit, dass nach demselben der Ausdruck:

$$\mathfrak{b}^{\mathfrak{s}} \mathfrak{c}^{\mathfrak{r}}$$

für alle Verbindungen β, γ , deren Anzahl:

$$(r^2-1)^{r^{g-1}} \cdot r^{g-1} = (r^2-1)^{r^{2g-2}} = \psi(r^g)$$

ist, lauter nach dem Modul r^g incongruente Zahlen darstellt, d. h. jeder nicht durch r theilbaren Zahl n einmal und nur einmal congruent wird.

Die Werthe β, γ , für welche dies geschieht, sollen die Indices von n heissen und mit β_n, γ_n bezeichnet werden. Offenbar haben congruente Zahlen dieselben Indices, und man sieht leicht, wie die Indices eines Productes aus denen der Factoren abzuleiten sind.

Da $c \equiv 1 \pmod{r}$ ist, so folgt aus:

$$b^{\beta_n} c^{\gamma_n} \equiv n \pmod{r^{\alpha}}$$

sgleich:

$$b^{\beta_n} \equiv n \pmod{r},$$

und dann, da b offenbar quadratischer Nichtrest von r ist, dass β_n gerade oder ungerade sein wird, je nachdem n quadratischer Rest oder Nichtrest von r ist, oder mit Anwendung des schon oben gebrauchten Zeichens:

$$(6) \quad \left[\frac{n}{r} \right] = (-1)^{\beta_n}.$$

III. Es bleibt uns noch der Fall zu untersuchen, wo der Modul eine Potenz von $1+i$ ist.

Es seien z und e zwei positive Zahlen, von denen die letztere als ungerade vorausgesetzt wird, und ausserdem sei t eine beliebige complexe ungerade Zahl. Da:

$$(1+t(1+i)^z)^e = 1+et(1+i)^z+\dots$$

ist und offenbar alle Glieder auf der rechten Seite, vom dritten an, durch $(1+i)^{z+1}$ theilbar sind, so folgt, dass $(1+t(1+i)^z)^e$ die Form $1+t'(1+i)^z$ haben wird, wo t' wieder ungerade ist. Ferner ist, wenn man $z \geq 3$ annimmt:

$$(1+t(1+i)^z)^2 = 1+t'(1+i)^{z+2},$$

wo t' ebenfalls ungerade ist. Wenn man diese beiden Resultate mit einander verbindet, so findet man ohne Schwierigkeit, dass — immer unter der Voraussetzung $z \geq 3$ — die Gleichung:

$$(1+t(1+i)^z)^{\varrho} = 1+t'(1+i)^{z+2\varrho}$$

besteht, in welcher t' wie t ungerade ist und ϱ den Exponenten der höchsten in \mathcal{G} aufgehenden Potenz von 2 bezeichnet.

Zu unserem Zwecke reicht es hin, wenn der Exponent der als Modul zu betrachtenden Potenz von $1+i$ ungerade und ≥ 7 ist. Es sei daher der Modul:

$$(1+i)^{3+2h},$$

so dass $h \geq 2$ ist. Setzt man in dem vorher erhaltenen Resultate $z = 3$ oder $z = 4$, so sieht man sogleich, dass $1+t(1+i)^z$ für den Modul $(1+i)^{3+2h}$ zum Exponenten 2^h gehört. Dies vorausgesetzt, ist es leicht sich zu überzeugen, dass die beiden zum Exponenten 2^h gehörigen Zahlen $1+t(1+i)^3$ und $1+u(1+i)^4$, in denen t und u ungerade sind, immer die Eigenschaft besitzen, dass die

Congruenz:

$$(1+t(1+i)^3)^{\delta} \equiv (1+u(1+i)^4)^{\varepsilon} \pmod{(1+i)^{3+2h}},$$

wenn man darin unter δ und ε aus der Reihe 0, 1, 2, . . . , $2^h - 1$ zu nehmende Zahlen versteht, nur für den Fall bestehen kann, wo:

$$\delta = \varepsilon = 0$$

ist. In der That, da offenbar jede der Voraussetzungen $\delta = 0$, $\varepsilon = 0$ die andere zur Folge hat, so haben wir nur noch nachzuweisen, dass unsere Congruenz unmöglich wird, wenn δ und ε beide von der Null verschieden sind.

Bezeichnet man mit 2^{ϱ} und 2^{σ} die höchsten in δ und ε resp. aufgehenden Potenzen von 2, wo $\varrho < h$, $\sigma < h$, so werden die beiden Seiten resp. in den beiden Formen:

$$1+t'(1+i)^{3+2\varrho}, \quad 1+u'(1+i)^{4+2\sigma}$$

enthalten sein, worin t' und u' ungerade Zahlen bezeichnen. Setzt man diese Werthe ein, so kommt:

$$t'(1+i)^{3+2\varrho} \equiv u'(1+i)^{4+2\sigma} \pmod{(1+i)^{3+2h}},$$

welche Congruenz offenbar unmöglich ist, da die Exponenten $3+2\varrho$ und $4+2\sigma$ ungleich und beide kleiner als $3+2h$ sind.

Setzt man speciell $t = 1$, $u = -1$, so kann also die Congruenz:

$$(-1+2i)^{\delta} \equiv 5^{\varepsilon} \pmod{(1+i)^{3+2h}}$$

nur unter der Voraussetzung stattfinden, dass man $\delta = \varepsilon = 0$ habe, oder, was, wie man sich leicht überzeugt, auf dasselbe hinauskommt, der Ausdruck:

$$(-1+2i)^{\delta} 5^{\varepsilon}$$

stellt für alle Verbindungen δ , ε , deren Anzahl offenbar 2^{2h} beträgt, lauter nach dem Modul $(1+i)^{3+2h}$ incongruente Zahlen dar. Alle diese Zahlen sind primär, d. h. congruent 1 $\pmod{(1+i)^2}$, da $-1+2i$ und 5 selbst diese Eigenschaft besitzen. Erwägt man nun, dass offenbar für jeden durch $(1+i)^2$ theilbaren Modul zwei congruente ungerade Zahlen immer gleichzeitig primär oder nicht primär sind, und dass folglich unser Ausdruck nur primären Zahlen congruent werden kann, und bemerkt man ferner, dass für den Modul $(1+i)^{3+2h}$, wie leicht zu sehen ist, nur $\frac{1}{4}\psi((1+i)^{3+2h}) = 2^{2h}$ ungerade primäre Zahlen existiren, die unter einander incongruent sind, so sieht man, dass der obige Ausdruck

jeder ungeraden primären Zahl n einmal und nur einmal congruent wird. Die Exponenten δ_n, ϵ_n , für welche dies geschieht, sollen wieder die Indices von n heissen, und es leuchtet ein, dass man den ersten oder zweiten Index eines Productes findet, indem man von der Summe der ersten oder zweiten Indices der Factoren das grösste darin enthaltene Vielfache von 2^b abzieht.

Die Indices δ_n, ϵ_n besitzen wieder Eigenschaften, welche den am Schlusse der beiden vorhergehenden Nummern bemerkten analog sind und sich wie diese auf die Theorie der quadratischen Reste beziehen. Setzt man:

$$(-1+2i)^{\delta_n} 5^{\epsilon_n} = \lambda' + \nu' i,$$

wo λ' und ν' resp. ungerade und gerade sind, so hat man nach dem in der angeführten Abhandlung (§. 8, Gleichung (c) und (f)) Bewiesenen¹⁾:

$$(-1)^{\frac{\lambda'^2 + \nu'^2 - 1}{4}} = \left[\frac{i}{\lambda' + \nu' i} \right] = \left[\frac{i}{-1+2i} \right]^{\delta_n} \left[\frac{i}{5} \right]^{\epsilon_n}.$$

$$(-1)^{\frac{(\lambda' + \nu')^2 - 1}{8}} = \left[\frac{1+i}{\lambda' + \nu' i} \right] = \left[\frac{1+i}{-1+2i} \right]^{\delta_n} \left[\frac{1+i}{5} \right]^{\epsilon_n}.$$

und folglich, da:

$$\left[\frac{i}{-1+2i} \right] = -1, \quad \left[\frac{i}{5} \right] = 1, \quad \left[\frac{1+i}{-1+2i} \right] = 1, \quad \left[\frac{1+i}{5} \right] = -1$$

ist:

$$(-1)^{\frac{\lambda'^2 + \nu'^2 - 1}{4}} = (-1)^{\delta_n}, \quad (-1)^{\frac{(\lambda' + \nu')^2 - 1}{8}} = (-1)^{\epsilon_n}.$$

Wird nun $n = \lambda + \nu i$ gesetzt, und bemerkt man, dass wegen:

$$\lambda + \nu i \equiv \lambda' + \nu' i \pmod{8},$$

welche letztere Congruenz daraus folgt, dass 8 ein Factor von $(1+i)^{3+2h}$ ist, λ und ν resp. von λ' und ν' um Vielfache von 8 verschieden sind, so sieht man sogleich, dass in den zuletzt erhaltenen Gleichungen λ', ν' mit λ, ν vertauscht werden können, und man erhält:

$$(7) \quad n = \lambda + \nu i, \quad (-1)^{\frac{\lambda^2 + \nu^2 - 1}{4}} = (-1)^{\delta_n}, \quad (-1)^{\frac{(\lambda + \nu)^2 - 1}{8}} = (-1)^{\epsilon_n}.$$

IV. Wir sind jetzt im Stande, eine beliebige Zahl k als Modul zu betrachten; um jedoch jede unnütze Weitläufigkeit zu vermeiden, beschränken wir uns auf den Fall, wo k gerade ist, die höchste darin aufgehende Potenz von $1+i$ einen Exponenten der Form $3+2h$ hat und $h \geq 2$ ist. Die Zahl k sei,

¹⁾ S. 559 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

abgesehen von dem Factor i^a , das Product der Primzahlpotenzen:

$$(8) \quad (a+bi)^f, (a'+b'i)^f, \dots; \quad r^g, r'^g, \dots; \quad (1+i)^{3+2h}.$$

Die ungeraden und zweigliedrigen Primzahlen $a+bi, a'+b'i, \dots$, welche zu grösserer Einfachheit primär vorausgesetzt werden, sind ungleich, und r, r', \dots sind eingliedrige, positive, ebenfalls von einander verschiedene Primzahlen.

Wählt man nun für jeden der Moduln (8) nach den Vorschriften der drei vorhergehenden Nummern eine oder zwei Basen:

$$(9) \quad \text{a. } a', \dots; \quad \text{b. } c, b', c', \dots; \quad -1+2i, 5,$$

so erhält man für jedes n , welches relative Primzahl zu k und zugleich primär ist, eine Reihe von Indices:

$$(10) \quad \alpha_n, \alpha'_n, \dots; \quad \beta_n, \gamma_n, \beta'_n, \gamma'_n, \dots; \quad \delta_n, \varepsilon_n,$$

welche *das System der Indices von n* heissen soll und völlig bestimmt ist, wenn die Basen ein für allemal gewählt sind. Dass congruente Zahlen n und n' dasselbe System der Indices haben, ist klar, und dass auch der umgekehrte Satz stattfindet, geht daraus hervor, dass bei vorausgesetzter Identität der Systeme für zwei Zahlen n und n' , die Congruenz $n \equiv n'$ für jeden der Moduln (8) und folglich auch für den Modul k besteht. Berücksichtigt man die Anzahl der Werthe, die den einzelnen Indices (10) zukommen können, so sieht man so gleich, dass die Anzahl der verschiedenen Systeme (10) durch das Product:

$$(p-1)p^{f-1} \cdot (p'-1)p'^{f'-1} \dots \times (r^2-1)r^{2g-2} \cdot (r'^2-1)r'^{2g'-2} \dots \times 2^{2h},$$

d. h. durch $\frac{1}{4}\psi(k)$ ausgedrückt wird, wie dies auch in der That der Fall sein muss, da $\frac{1}{4}\psi(k)$ offenbar mit der Anzahl aller nach dem Modul k incongruenten Zahlen, welche mit diesem keinen gemeinschaftlichen Factor haben und überdies primär sind, zusammenfällt.

Da wir in den folgenden Paragraphen häufig eine Reihe von Zahlen von der eben angegebenen Beschaffenheit zu betrachten haben werden, d. h. eine Reihe, die ein und nur ein Glied enthält, welches jeder primären, zu k relativen Primzahl nach dem Modul k congruent ist, so wollen wir übereinkommen, mit:

$$(11) \quad l$$

das allgemeine Glied einer solchen aus $\frac{1}{4}\psi(k)$ Gliedern bestehenden Zahlenreihe zu bezeichnen.

§. 3.

Indem wir zu dem in der Einleitung als Gegenstand dieser Abhandlung bezeichneten Satze übergehen, nach welchem:

$$kt+l$$

immer unendlich viel Primzahlen enthält, wenn die gegebenen Zahlen k und l keinen gemeinsamen Theiler haben, bemerken wir zunächst, dass man offenbar, ohne der Allgemeinheit zu schaden, k als durch $1+i$ theilbar und den Exponenten der höchsten darin aufgehenden Potenz von $1+i$ als ungerade und ≥ 7 betrachten kann, so dass also k von der in §. 2, IV. vorausgesetzten Form sein wird. Erwägt man ferner, dass vier zusammengehörige Zahlen immer zugleich Primzahlen sind oder nicht sind, so leuchtet ein, dass man l als eine primäre Zahl ansehen kann, und dass daher auch dieser Buchstabe in der ihm unter (11) gegebenen Bedeutung genommen werden kann.

Dies vorausgesetzt, bilde man unter Beibehaltung aller in §. 2, IV. gebrauchten Bezeichnungen, den Basen (9) der Reihe nach entsprechend, die binomischen Gleichungen:

$$(12) \quad \begin{cases} g^{(p-1)p^{j-1}} = 1, & g^{t(p'-1)p'^{j-1}} = 1, \dots \\ \psi^{(r^2-1)r^{j-1}} = 1, & \chi^{r^{j-1}} = 1; & \psi^{(r'^2-1)r'^{j-1}} = 1, & \chi'^{r'^{j-1}} = 1; \dots \\ g^{2^h} = 1, & \eta^{2^h} = 1, \end{cases}$$

und setze ferner zur Abkürzung:

$$\Omega_n = g^{a_n} g^{t a'_n} \dots \times \psi^{\beta_n} \chi^{\gamma_n} \psi^{t \beta'_n} \chi'^{\gamma'_n} \dots \times \eta^{\delta_n} \eta^{\epsilon_n}.$$

Das so gebildete Product besitzt mehrere sehr leicht zu beweisende und für das Folgende wichtige Eigenschaften, welche vor allen Dingen zu betrachten sind.

Denkt man sich zunächst die in Ω enthaltenen Wurzeln der Einheit als constant, so hat man offenbar:

$$(13) \quad \Omega_{nn'} = \Omega_n \Omega_{n'},$$

und wenn $n' \equiv n \pmod{k}$ angenommen wird:

$$(13') \quad \Omega_{n'} = \Omega_n.$$

Ferner ist, immer unter der Voraussetzung, dass man die in Ω enthaltenen Wurzeln der Einheit nicht ändert, und wenn das Zeichen Σ sich auf alle unter

(11) definirten Werthe von l erstreckt:

$$(14) \quad \Sigma \Omega_i = 0, \quad \text{oder} \quad \Sigma \Omega_i = \frac{1}{4} \psi(k),$$

je nachdem unter den Wurzeln $g, g', \dots, \psi, \chi, \psi', \chi', \dots, \vartheta, \eta$ wenigstens eine von der positiven Einheit verschiedene sich befindet oder alle dieser gleich sind. In der That lässt sich unsere Summe, da allen l alle möglichen Systeme (10) entsprechen, leicht in Factoren zerlegen, von denen jeder nur eine der oben genannten Wurzeln enthält. Derjenige dieser Factoren, in welchem g vorkommt, ist offenbar:

$$1 + g + g^2 + \dots + g^{(p-1)p^{f-1}-1}$$

und folglich gleich 0 oder gleich $(p-1)p^{f-1}$, je nachdem g von der positiven Einheit verschieden oder derselben gleich ist, und da Ähnliches von allen übrigen gilt, so ist die ausgesprochene Behauptung bewiesen.

Wenn wir uns jetzt, wie überall im Folgenden, des Zeichens S bedienen, um eine Summation anzudeuten, welche sich über alle Combinationen der Wurzeln der Gleichungen (12) erstreckt, deren Anzahl offenbar gleich $\frac{1}{4} \psi(k)$ ist, so hat man endlich:

$$(15) \quad S \Omega_n = \frac{1}{4} \psi(k), \quad \text{oder} \quad S \Omega_n = 0,$$

je nachdem $n \equiv 1$ oder nicht $\equiv 1 \pmod{k}$ ist.

Das erste Resultat folgt unmittelbar daraus, dass für $n \equiv 1$ alle Indices (10) verschwinden. Um sich von der Richtigkeit des zweiten zu überzeugen, darf man nur bemerken, dass $S \Omega_n$ in Factoren zerlegt werden kann, von denen jeder nur die Wurzeln einer der Gleichungen (12) enthält, und dass der auf die erste dieser Gleichungen sich beziehende nichts anderes ist als die Summe der a_n^{ten} Potenzen aller Wurzeln dieser Gleichung. Dieser Factor wird daher und wegen $a_n < (p-1)p^{f-1}$ immer verschwinden, ausser wenn $a_n = 0$ ist. Aus diesem und den ähnlichen Resultaten, welche für die übrigen Factoren gelten, folgt die zweite der Gleichungen (15) sogleich, wenn man berücksichtigt, dass, wenn n nicht $\equiv 1 \pmod{k}$ ist, wenigstens einer der Indices (10) von Null verschieden sein wird.

Nach den bisher getroffenen Einleitungen können wir ohne Schwierigkeit die Gleichung:

$$(16) \quad H - \frac{1}{1 - \Omega_g} \frac{1}{(\Delta g)^s} = \Sigma \Omega_n \frac{1}{(\Delta n)^s} = L$$

beweisen. In dieser Gleichung bedeutet s eine beliebige positive, die Einheit übertreffende Grösse, und was das Multiplicationszeichen Π und das Summationszeichen Σ betrifft, so erstreckt sich ersteres über alle primären Primzahlen q , welche nicht in k aufgehen, während letzteres auf alle primären Zahlen n auszudehnen ist, die mit k keinen gemeinsamen Theiler haben. Die in Ω eingehenden Wurzeln q, q', \dots können beliebig gewählt werden, müssen aber in jedem Ω dieselben sein, so dass also unsere allgemeine Gleichung $\frac{1}{4}\psi(k)$ besondere, den verschiedenen Wurzelverbindungen entsprechende Gleichungen darstellt.

Um sich von der Richtigkeit der Gleichung (16) zu überzeugen, entwickle man den allgemeinen Factor auf der ersten Seite mit Berücksichtigung der Gleichung (13). Man erhält so:

$$\frac{1}{1 - \Omega_q \frac{1}{(Nq)^s}} = 1 + \Omega_q \frac{1}{(Nq)^s} + \Omega_{q^2} \frac{1}{(Nq^2)^s} + \dots$$

Führt man nun die auf der ersten Seite der Gleichung (16) angedeutete Multiplication aus und erinnert sich, dass nach (4) jede Zahl n nur auf eine Weise als ein Product von Potenzen primärer Primzahlen dargestellt werden kann, so wird die erste Seite unserer Gleichung in die zweite übergehen, w. z. b. w.

§. 4.

Wir müssen jetzt die allgemeine Reihe $L(16)$, welche, wie leicht zu sehen, so lange $s > 1$ ist, einen endlichen, von der Art der Aufeinanderfolge ihrer Glieder unabhängigen Werth hat, näher betrachten und namentlich auszumitteln suchen, wie sich dieser Werth ändert, wenn man, $s = 1 + \varrho$ setzend, die positive Variable ϱ unendlich klein werden lässt. Die zu untersuchende Reihe L zerfällt in $\frac{1}{4}\psi(k)$ Partialreihen, von denen jede alle diejenigen Glieder enthält, für welche n derselben Zahl l (11) nach dem Modul k congruent ist. Irgend eine solche Partialreihe ist, wenn man von dem allen ihren Gliedern gemeinsamen Factor Ω abstrahirt:

$$W = \Sigma \frac{1}{N(kt+l)^{s+\varrho}}$$

wo sich das Zeichen Σ auf alle complexen ganzen Zahlen l bezieht. Nun ist in der Abhandlung¹⁾ *Recherches sur les formes quadratiques à coefficients et à*

¹⁾ S. 533 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

indéterminées complexes (§. 18, II.) gezeigt worden, dass letztere Reihe für ein unendlich kleines ϱ dem Ausdruck $\frac{\pi}{N(k)} \frac{1}{\varrho}$ gleich wird. Dieses Resultat lässt sich mit Hilfe der am angeführten Orte entwickelten Betrachtungen vervollständigen, und man beweist leicht, dass:

$$W = \frac{\pi}{N(k)} \frac{1}{\varrho} + A + \varrho F(\varrho)$$

ist, wo A eine reelle Constante und $F(\varrho)$ eine reelle Function von ϱ bezeichnet, die sich für ein unendlich klein werdendes ϱ einer endlichen Grenze nähert. Hieraus folgt sogleich mit Berücksichtigung von (14), dass:

$$(17) \quad L = \frac{\pi \psi(k)}{4N(k)} \frac{1}{\varrho} + F(\varrho), \quad \text{oder} \quad L = A + A'i + \varrho(\Phi(\varrho) + i\Phi'(\varrho))$$

ist, je nachdem die in L enthaltenen Wurzeln der Einheit alle der positiven Einheit gleich sind oder wenigstens eine derselben von dieser verschieden ist. A und A' sind reelle Constanten und $F(\varrho)$, $\Phi(\varrho)$, $\Phi'(\varrho)$ reelle Functionen von ϱ , die für einen unendlich kleinen Werth der positiven Veränderlichen ϱ sich endlichen Grenzen nähern.

Die Reihen L zerfallen nach den verschiedenen in ihnen enthaltenen Wurzelcombinationen in folgende drei Classen. Die erste dieser Classen besteht aus der einzigen Reihe, in welcher alle Wurzeln der Einheit den Werth 1 haben, und auf welche sich die erste der Gleichungen (17) bezieht. Die zweite Classe umfasst alle übrigen Reihen, in denen nur reelle Wurzeln vorkommen. Bemerkt man nun, dass nur in denjenigen der Gleichungen (12), deren Wurzeln mit χ , χ' , ... bezeichnet sind, die Exponenten ungerade sind, so sieht man, dass zur Darstellung aller Reihen der zweiten Classe die doppelten Zeichen in:

$g = \pm 1$, $g' = \pm 1$, ...; $\psi = \pm 1$, $\chi = 1$, $\psi' = \pm 1$, $\chi' = 1$, ...; $\vartheta = \pm 1$, $\eta = \pm 1$ auf jede mögliche Weise combinirt werden müssen, wobei nur die eine aus allen oberen Zeichen bestehende Verbindung als der ersten Classe entsprechend ausgeschlossen bleiben muss. Die dritte Classe endlich wird alle Reihen in sich begreifen, in denen wenigstens eine imaginäre Wurzel der Einheit vorkommt, und man sieht ohne Schwierigkeit, dass die Reihen dieser Classe immer paarweise einander zugeordnet sind, indem, unter der ausgesprochenen Voraussetzung, die beiden Wurzelcombinationen:

$$g, g', \dots; \psi, \chi, \psi', \chi', \dots; \vartheta, \eta \quad \text{und} \quad \frac{1}{g}, \frac{1}{g'}, \dots; \frac{1}{\psi}, \frac{1}{\chi}, \frac{1}{\psi'}, \frac{1}{\chi'}, \dots; \frac{1}{\vartheta}, \frac{1}{\eta}$$

offenbar von einander verschieden sind. Bei diesen Reihen findet der Übergang von einer derselben zu der ihr zugeordneten statt, wenn man in der zweiten Gleichung (17) i mit $-i$ vertauscht, während für die Reihen der zweiten Classe, für welche die erwähnte Gleichung ebenfalls gilt, die in dieser Gleichung vorkommenden imaginären Glieder verschwinden.

Wird q unendlich klein, so wächst der Werth der die erste Classe L constituirenden Reihe über jede positive Grenze hinaus, während die Werthe aller übrigen sich endlichen Grenzen nähern, wie aus (17) ersichtlich. Dies ist jedoch zu unserem Zwecke nicht ausreichend, und wir müssen nachweisen, dass alle diese Grenzen von Null verschieden sind, d. h. dass in der zweiten der Gleichungen (17) nie gleichzeitig $A = 0$, $A' = 0$ ist. Wir wollen für einen Augenblick annehmen, dieser Nachweis sei für alle Reihen der zweiten Classe geführt. Unter dieser Voraussetzung soll im folgenden Paragraphen die Richtigkeit derselben Behauptung für die dritte Classe gezeigt und zugleich der am Anfang des §. 3 aufgestellte Satz abgeleitet werden, so dass uns dann nur noch übrig bleiben wird, am Schlusse der Abhandlung die hinsichtlich der Reihen der zweiten Classe vorausgesetzte Eigenschaft zu beweisen.

§. 5.

Nimmt man von beiden Seiten der Gleichung (16) die NEPER'schen Logarithmen und entwickelt, so kommt:

$$\dots + \frac{1}{\mu} \Sigma \Omega_q^\mu \frac{1}{(Nq)^{\mu+\mu q}} + \dots = \log L,$$

wo wir zur Abkürzung nur das allgemeine Glied geschrieben haben, in welchem für μ successive alle Werthe von $\mu = 1$ bis $\mu = \infty$ zu setzen sind, und wo sich das Summenzeichen auf alle q erstreckt.

Es sei nun l irgend eine bestimmte der unter (11) definirten Zahlen, und man setze $l' = 1 \pmod{k}$, wo l' , wie l , primär und Primzahl zu k ist. Multiplicirt man unsere Gleichung mit $\Omega_{l'}$ und summirt nach allen Wurzelverbindungen, so erhält man:

$$\dots + \frac{1}{\mu} \Sigma (S \Omega_{l' q}^\mu) \frac{1}{(Nq)^{\mu+\mu q}} + \dots = S \Omega_{l'} \log L.$$

Nun ist, nach (15):

$$S \Omega_{l' q}^\mu = 0,$$

ausser wenn $l'q^u \equiv 1$ oder, was dasselbe ist, ausser wenn $q^u \equiv l \pmod{k}$ ist, für welchen Fall:

$$S\Omega_{l'q^u} = \frac{1}{4}\psi(k)$$

ist. Die Gleichung wird daher:

$$(18) \quad \Sigma \frac{1}{(Nq)^{l+e}} + \frac{1}{2}\Sigma \frac{1}{(Nq)^{2+2e}} + \dots = \frac{4}{\psi(k)} S\Omega_l \log L,$$

wo sich das Zeichen Σ im ersten, zweiten, . . . Gliede resp. auf die Primzahlen q erstreckt, deren erste, zweite, . . . Potenzen congruent $l \pmod{k}$ sind. Setzt man speciell $l \equiv 1$, so ist:

$$l' \equiv 1 \pmod{k}, \quad \Omega_l = 1,$$

und das allgemeine Resultat geht über in:

$$\Sigma \frac{1}{(Nq)^{l+e}} + \frac{1}{2}\Sigma \frac{1}{(Nq)^{2+2e}} + \dots = \frac{4}{\psi(k)} S\log L.$$

Wir betrachten jetzt die Summe $S\log L$ für den Fall, wo q unendlich klein wird. Was zunächst die den Reihen der zweiten Classe entsprechenden Glieder betrifft, so werden sich diese sämmtlich endlichen Grenzen nähern, wogegen das der ersten Classe entsprechende Glied einen unendlich grossen positiven Werth annimmt, indem dasselbe nach (17) in die Form:

$$\log\left(\frac{1}{q}\right) + \log\left(\frac{\pi\psi(k)}{4N(k)} + eF(q)\right)$$

gebracht werden kann, wo der erste Theil unendlich wird, während der zweite sich einer endlichen Grenze nähert. Wäre nun der endliche Grenzwert einer Reihe der dritten Classe der Null gleich, d. h. wäre in (17) $A = 0$, $A' = 0$, so würde sich aus der Vereinigung der zwei Glieder, welche in unserer Summe dieser und der ihr zugeordneten Reihe entsprechen, der Ausdruck:

$$-2\log\left(\frac{1}{q}\right) + \log(\Phi(q)^2 + \Phi'(q)^2)$$

ergeben, nach dessen Verbindung mit dem eben betrachteten die Summe das Glied:

$$-\log\left(\frac{1}{q}\right)$$

darbieten würde, welches einen unendlich grossen negativen Werth annimmt

und nicht etwa durch $\log(\Psi(\varrho)^2 + \Psi'(\varrho)^2)$ aufgehoben werden kann, indem dieser letztere Logarithmus sich entweder einer endlichen Grenze nähert oder selbst einen unendlich grossen negativen Werth erhält. Dies widerspricht unserer obigen Gleichung, deren linke Seite nur positive Glieder enthält, und der hier hervortretende Widerspruch würde offenbar noch verstärkt werden, wenn man die Grenzwerte für mehr als ein Paar zugeordneter Reihen der dritten Classe als verschwindend betrachten wollte. Es ist somit, unter Vorbehalt des noch zu leistenden Nachweises für die Reihen der zweiten Classe, bewiesen, dass $\log L$ sich immer einer endlichen Grenze nähert, den einzigen Fall ausgenommen, wenn L die Reihe der ersten Classe bezeichnet, da für diesen Fall unser Logarithmus über jede positive noch so grosse Zahl hinaus wächst.

Kehren wir jetzt zur allgemeinen Gleichung (18) zurück, so sehen wir, dass die rechte und also auch die linke Seite derselben für ein unendlich klein werdendes ϱ unendlich wird. Nun bleibt aber die Summe aller auf der linken Seite vorkommenden Reihen, von der zweiten ab, endlich, da, wie leicht zu sehen:

$$\frac{1}{2} \sum \frac{1}{(Nq)^2} + \frac{1}{3} \sum \frac{1}{(Nq)^3} + \dots$$

noch endlich ist, wenn man die Summationen nicht, wie es hier geschieht, auf gewisse Primzahlen q beschränkt, sondern auf alle ganzen Zahlen, deren Norm die Einheit übertrifft, ausdehnt. Es muss daher die Summe:

$$\sum \frac{1}{(Nq)^{1+e}}$$

über jede endliche Grenze hinaus wachsen, was nicht anders geschehen kann, als wenn die Gliederzahl derselben unendlich ist, d. h. als wenn es eine unendliche Anzahl von Primzahlen giebt, die in der Form $kt+l$ enthalten sind, w. z. b. w.

§. 6.

Zur Vervollständigung des eben gegebenen Beweises ist noch zu zeigen, dass der einem unendlich kleinen ϱ entsprechende Grenzwert jeder Reihe der zweiten Classe von Null verschieden ist. Eine solche Reihe enthält eine Wurzelverbindung der Form:

$$g = \pm 1, g' = \pm 1, \dots; \psi = \pm 1, \chi = 1, \psi' = \pm 1, \chi' = 1, \dots; \vartheta = \pm 1, \vartheta' = \pm 1,$$

Bildet man das Product aller derjenigen der Primzahlen $a + bi, a' + b'i, \dots$,

r, r', \dots denen in dieser Wurzelcombination eine der negativen Einheit gleiche Wurzel $g, g', \dots, \psi, \psi', \dots$ entspricht, und bezeichnet das Product dieser Primzahlen mit Q , so wie das aller übrigen mit V (wobei es sich von selbst versteht, dass, wenn in einer dieser Gruppen keine Primzahl vorkommen sollte, man für Q oder V die Einheit zu wählen hat), so wird der im allgemeinen Gliede der Reihe enthaltene Ausdruck Ω_n nach den unter (5) und (6) erhaltenen Resultaten folgende Gestalt annehmen können:

$$\Omega_n = \left[\frac{n}{Q} \right] g^{\delta_n} \eta^{\epsilon_n}.$$

Setzt man ferner, wie oben, $n = \lambda + \nu i$, so hat man:

$$g^{\delta_n} = g^{\frac{\lambda^2 + \nu^2 - 1}{4}}, \quad \eta^{\epsilon_n} = \eta^{\frac{(\lambda + \nu)^2 - 1}{8}}.$$

Ist $\vartheta = 1$, so ist die erste dieser Gleichungen evident; ist dagegen $\vartheta = -1$, so fällt sie mit einer der unter (7) bewiesenen zusammen, und mit der zweiten verhält es sich ebenso. Der Grenzwertb irgend einer Reihe der zweiten Classe ist folglich:

$$\Sigma g^{\frac{\lambda^2 + \nu^2 - 1}{4}} \eta^{\frac{(\lambda + \nu)^2 - 1}{8}} \left[\frac{\lambda + \nu i}{Q} \right] \frac{1}{(\lambda^2 + \nu^2)^{1+e}}.$$

wenn q unendlich klein vorausgesetzt ist, das Zeichen Σ sich über alle ungeraden primären Zahlen $\lambda + \nu i$ erstreckt, die mit k oder, was dasselbe ist, mit QV keinen Factor gemein haben, und noch zu bemerken ist, dass nicht gleichzeitig $Q = 1, \vartheta = 1, \eta = 1$ sein kann, da unter dieser Voraussetzung die oben betrachtete Wurzelcombination der Reihe L der ersten Classe entsprechen würde. Nun ist aber unsere Reihe mit der eben angegebenen Beschränkung immer in der allgemeinen Reihe enthalten, welche, wie wir in der schon oft citirten Abhandlung¹⁾ gezeigt haben, von einem endlichen Factor abgesehen, die Anzahl der Classen ausdrückt, in welche sich alle quadratischen Formen für eine beliebige, keinem Quadrat gleiche, Determinante vertheilen. Vergleicht man die in jener Abhandlung (§. 18. IV. Gleichung (18)) zur Bestimmung dieser Anzahl gefundene Reihe mit der obigen, so sieht man, dass letztere sich nach den vier Wurzelverbindungen:

$$\vartheta = 1, \quad \eta = 1; \quad \vartheta = -1, \quad \eta = 1; \quad \vartheta = 1, \quad \eta = -1; \quad \vartheta = -1, \quad \eta = -1,$$

¹⁾ S. 533 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

welche darin vorkommen können, resp. auf die vier Determinanten:

$$QI^2, \quad iQI^2, \quad (1+i)QI^2, \quad i(1+i)QI^2$$

bezieht.

Hieraus folgt die zu beweisende Eigenschaft sogleich; denn wenn unsere Reihe sich auf Null reducirte, so würde auch die Anzahl der Classen der quadratischen Formen für die entsprechende Determinante verschwinden, was nicht möglich ist, indem diese Anzahl immer wenigstens der Einheit gleich ist.

Wir schliessen mit einer die vorher erwähnte Vergleichung erleichternden Bemerkung, welche darin besteht, dass man in der am angeführten Orte gefundenen Reihe, ohne den Werth derselben zu ändern, die Summation auf diejenigen ungeraden, mit der Determinante keinen gemeinschaftlichen Factor darbietenden, primären Zahlen $\lambda + \nu i$ beziehen kann, denen diese Benennung in dem in gegenwärtiger Abhandlung angenommenen Sinne zukommt. Dies ergibt sich unmittelbar daraus, dass für irgend eine Gruppe ungerader zusammengehöriger Zahlen, die nach der einen Definition als primär zu betrachtende Zahl derjenigen, welche der anderen Definition entspricht, offenbar gleich oder entgegengesetzt ist, und dann ferner daraus, dass irgend ein Glied der Reihe ungeändert bleibt, wenn man darin $\lambda + \nu i$ mit $-\lambda - \nu i$ vertauscht.

RECHERCHES
SUR LES FORMES QUADRATIQUES
A COEFFICIENTS ET A INDÉTERMINÉES COMPLEXES.

PAR

M. G. LEJEUNE DIRICHLET.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 24 p. 291—371.

RECHERCHES
SUR LES FORMES QUADRATIQUES
A COEFFICIENTS ET A INDÉTERMINÉES COMPLEXES.

Première partie.

Comme les recherches que nous aurons à exposer dans ce Mémoire, présentent, par leur objet et par les résultats auxquels elles conduisent, beaucoup d'analogie avec d'autres recherches déjà publiées^{*)}, il convient, avant d'en donner une idée générale, de rappeler en peu de mots la question qui a été traitée dans le Mémoire que nous venons de citer. Le Mémoire dont il s'agit, se rapporte à la théorie des *formes quadratiques*, théorie qui, préparée par quelques énoncés de FERMAT et par les ingénieuses recherches d'EULER et définitivement fondée par LAGRANGE, a reçu plus tard de notables accroissements par les travaux de LEGENDRE et surtout par ceux de M. GAUSS, qui y a consacré la plus grande partie de ses *„Disquisitiones arithmeticae“*, en sorte qu'elle constitue aujourd'hui l'une des branches principales de la science des nombres. On sait que les propriétés d'une telle expression dépendent surtout d'un entier qui est une fonction très simple de ses coefficients et que, pour cette raison, on nomme le *déterminant* de la forme quadratique. Quoique le nombre des formes qui ont un même déterminant donné quelconque, positif ou négatif, soit infini, ces formes se réduisent toujours à un nombre limité d'expressions distinctes, c'est-à-dire non-transformables les unes dans les autres. Cette propriété, capitale dans la matière, a été établie par LAGRANGE qui a aussi fait connaître les opérations arithmétiques, au moyen desquelles ces formes non-équivalentes peuvent être assignées, lorsque le déterminant est numériquement donné. Mais si ce procédé suffisait pour l'objet auquel son illustre auteur l'avait destiné, il ne donnait aucune lumière sur la liaison générale qui doit exister

^{*)} Recherches sur diverses applications de l'Analyse infinitésimale à la Théorie des Nombres, Tome XIX et XXI du Journal de CRELLE¹⁾.

¹⁾ S. 411 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

entre le déterminant et le nombre des formes distinctes qui y répondent. La loi qui exprime cette dépendance et dont la connaissance, outre qu'elle devait présenter beaucoup d'intérêt par elle-même, était indispensable pour d'autres recherches, restait donc entièrement inconnue. Or tel est précisément l'objet de la question qu'on s'est proposée dans le Mémoire cité et qu'on y a résolu au moyen d'une analyse dont le principe fondamental consiste à exprimer les propriétés caractéristiques du système des formes non-équivalentes répondant à un déterminant quelconque, à l'aide d'une équation dont l'un des membres ne contient rien qui soit relatif à ces formes, tandis que l'autre se compose de suites infinies doubles dont le nombre est égal à celui des formes et dont chacune présente dans son terme général l'une des expressions quadratiques dont il s'agit. L'équation ainsi formée renfermant une variable assujettie à la seule condition de rester supérieure à l'unité, si l'on passe au cas-limite, où cette variable approche indéfiniment de l'unité, les séries doubles tendent toutes vers une limite commune facile à assigner, et l'égalité se transforme de manière à exprimer le nombre des formes par une suite infinie d'une loi très simple et dont la somme s'obtient aisément avec le secours des formules connues. En effectuant cette dernière opération, on reconnaît que l'expression du nombre des formes qui répondent à un déterminant quelconque, présente deux cas très distincts suivant que ce déterminant est un nombre négatif ou positif. Dans le premier de ces cas, l'expression de la loi dont il s'agit a un caractère purement arithmétique, tandis que pour un déterminant positif elle est d'une nature plus composée et en quelque sorte mixte, puisque, outre les éléments arithmétiques dont elle dépend, elle en renferme d'autres qui ont leur origine dans certaines équations auxiliaires qui se présentent dans la théorie des équations binômes, et appartiennent par conséquent à l'Algèbre. Ce dernier résultat est surtout remarquable et offre un nouvel exemple de ces rapports cachés que l'étude approfondie de l'Analyse mathématique nous fait découvrir entre les questions en apparence les plus disparates.

La solution dont nous venons de rappeler l'idée fondamentale, n'empruntant de la théorie des formes quadratiques que leurs propriétés les plus élémentaires et s'achevant sans difficulté, lorsque ces propriétés ont été une fois reconnues et mises en équation, il était naturel de chercher à étendre les applications de ce genre d'analyse et à résoudre par son moyen d'autres questions analogues mais d'un ordre plus élevé. Les questions que l'on doit considérer

comme telles, sont assez nombreuses; on peut, dans les recherches de cette nature, remplacer les formes quadratiques par des fonctions homogènes d'un degré plus élevé: sans sortir du second degré, et c'est là le cas dont nous nous sommes occupé d'abord et que nous traiterons exclusivement dans ce Mémoire, on peut aussi modifier la nature des formes quadratiques et supposer par exemple que leurs coefficients sont des entiers complexes. On doit à M. GAUSS l'idée de considérer de pareils entiers*), et l'on sait qu'il y a été conduit par ses recherches sur les résidus biquadratiques, qui lui ont fait reconnaître que la théorie de ces résidus qui paraît très compliquée tant qu'on la rapporte aux entiers réels, se présente sous une face bien différente, lorsqu'on l'envisage sous ce nouveau point de vue, et se résume alors dans une loi de réciprocité d'une simplicité et d'une élégance extrêmes et d'ailleurs parfaitement analogue à celle que l'on connaissait depuis longtemps pour les résidus quadratiques. L'importance de l'idée si profonde que nous venons de rappeler ne consiste pas seulement à amener de pareilles simplifications: elle est d'un usage beaucoup plus étendu et l'on doit la considérer comme ouvrant un nouveau champ aux spéculations arithmétiques.

Avant de transporter, dans la théorie des nombres ainsi généralisée, la question qui avait été traitée précédemment, il fallait se livrer à un travail préliminaire indispensable et ayant pour objet de se rendre compte des modifications que les propositions fondamentales de la théorie des formes quadratiques doivent subir pour être applicables aux entiers complexes. Ce travail achevé, on a pu reconnaître que les principes dont on avait fait usage dans le Mémoire cité, s'appliquent avec le même succès à la nouvelle question. Seulement, comme cette dernière est d'une nature plus compliquée, les discussions que la solution exige, prennent plus d'étendue et l'on trouve par exemple que pour passer à ce que nous avons nommé plus haut le cas-limite, il faut ici évaluer une intégrale définie quadruple, tandis que précédemment on n'avait eu à considérer que des intégrales doubles, se réduisant d'ailleurs sur-le-champ à la quadrature de l'ellipse ou de l'hyperbole.

Mais sans entrer ici dans d'autres détails sur la marche de la solution, nous nous bornerons à dire que le résultat définitif est entièrement semblable à celui qui répond au second des deux cas que nous avons distingués plus haut.

*) *Theoria residuorum biquadraticorum. Commentatio secunda.*

On reconnaît en effet que, pour un déterminant complexe, le nombre des formes se rattache généralement à la division de la fonction elliptique complète de première espèce dont le module est $\sqrt{\frac{1}{2}}$, ou ce qui revient au même, à la division de la lemniscate en parties égales, le diviseur ou le nombre de ces parties étant un entier complexe.

Outre le résultat dont nous venons d'indiquer la nature, la question présente deux résultats particuliers très singuliers et tout-à-fait inattendus. Ces résultats sont relatifs aux cas où le déterminant est un entier réel ou le produit d'un tel entier par $\sqrt{-1}$, le nombre des formes pouvant alors être assigné sans le secours des équations qui se rapportent à la division des fonctions elliptiques. Pour ne parler ici que du premier de ces deux cas dont le second ne diffère pas au fond, le résultat consiste en ce que, relativement à un entier réel D , considéré comme le déterminant de formes quadratiques à coefficients complexes, le nombre des formes distinctes est égal au produit ou au double produit des deux nombres qui expriment combien il existe de formes pour les deux déterminants opposés D et $-D$, considérés sous le point de vue ordinaire, ces deux cas étant d'ailleurs distingués par un critérium très simple.

Comme les recherches dont nous venons de présenter l'analyse, exigent des développements assez étendus, nous avons dû diviser notre travail en deux parties, dont la première que nous publions aujourd'hui, contient, outre les discussions préliminaires, la solution de la question principale conduite jusqu'au point où elle se trouve dépendre de la sommation d'une série double. Nous terminons cette première partie par l'examen des deux cas particuliers mentionnés plus haut, et qui peuvent être traités complètement, sans qu'il soit nécessaire d'effectuer la double sommation. Dans la seconde partie nous achèverons la solution générale et nous discuterons en outre quelques questions accessoires telles que celles qui concernent la distribution des formes quadratiques en genres, et que nous avons dû laisser de côté dans cette première partie, pour ne pas interrompre la marche des considérations qui se rapportent à la question principale.

Quoique les propositions élémentaires de la théorie des entiers complexes aient déjà été exposées par l'illustre géomètre que nous avons cité plus haut, nous avons pensé qu'il pourrait être commode pour le lecteur de trouver dans une courte introduction celles de ces propositions dont nous aurons à faire usage plus tard.

Définitions et théorèmes préliminaires.

§. 1.

On appelle *nombre complexe* toute expression de la forme:

$$a+bi,$$

i désignant la quantité imaginaire $\sqrt{-1}$, et a et b ayant des valeurs réelles quelconques. Comme il est souvent nécessaire de distinguer le cas où l'une des valeurs réelles a et b s'évanouit, de celui où ces valeurs sont l'une et l'autre différentes de zéro, nous nommerons l'expression précédente *monôme* ou *binôme* suivant ces deux cas.

Le nombre réel et toujours positif:

$$a^2+b^2,$$

le seul cas excepté où l'on a à la fois $a=0$, $b=0$, sera dit la *norme* du nombre complexe $a+bi$. Cette norme n'est donc autre chose que ce que l'on appelle communément le carré du module de l'expression imaginaire $a+bi$. Mais comme ce carré se présentera beaucoup plus souvent dans nos recherches que le module lui-même, il convient de lui consacrer une dénomination spéciale telle que la précédente déjà proposée par M. GAUSS, d'autant plus que l'emploi du mot *module* pourrait donner lieu à des équivoques.

Nous conviendrons de désigner la norme en plaçant la caractéristique N devant le nombre complexe dont il s'agit, et d'écrire:

$$N(a+bi).$$

Au moyen de ce signe on aura les équations évidentes et qu'on a souvent occasion d'employer:

$$N(kl) = N(k)N(l), \quad N\left(\frac{k}{l}\right) = \frac{N(k)}{N(l)}.$$

Dans la théorie des nombres complexes on a à considérer les quatre unités:

$$1, \quad i, \quad -1, \quad -i,$$

dont l'une quelconque peut être désignée par i^2 , en supposant $\varphi = 0, 1, 2, 3$.

On appelle nombres complexes associés quatre nombres:

$$a+bi, \quad -b+ai, \quad -a-bi, \quad b-ai,$$

dont chacun produit les trois autres, lorsqu'on le multiplie par i , -1 et $-i$. Ces quatre nombres sont toujours inégaux à moins qu'on n'ait simultanément $a=0$, $b=0$.

Deux nombres complexes:

$$a+bi, \quad a-bi$$

sont dits conjugués, l'un se changeant dans l'autre, en remplaçant i par $-i$. De pareils nombres sont toujours inégaux, excepté lorsque $b = 0$.

Des nombres associés ont une norme commune et la même chose a lieu pour deux nombres conjugués.

Ce qui précède s'applique à des nombres complexes quelconques.

Les nombres complexes $a+bi$ portent différents noms, suivant la nature des nombres réels a et b , qu'on en doit considérer comme leurs éléments. Un nombre complexe $a+bi$ s'appelle entier lorsque a et b sont l'un et l'autre des entiers, rationnel lorsque a et b sont l'un et l'autre rationnels, et irrationnel dans tout autre cas. Comme les nombres que nous aurons à considérer, seront presque toujours des nombres complexes entiers, nous supprimerons généralement les adjectifs à moins que cette suppression ne puisse donner lieu à des équivoques.

Lorsque relativement à un entier complexe k on a $N(k) = 1$, on peut en conclure: $k = i^e$. On voit encore par l'équation $N(kl) = N(k)N(l)$, que la norme d'un entier kl , multiple d'un autre l , est elle-même un multiple de celle de ce dernier. Il résulte de là que les diviseurs d'un entier quelconque m ont toujours des normes inférieures ou tout au plus égales à celle de m , et que ce dernier cas ne peut avoir lieu que lorsque le diviseur coïncide avec le nombre dont il s'agit ou avec l'un de ses trois associés.

Si donc, pour abrégé, on nomme plus grand qu'un autre un nombre complexe dont la norme surpasse celle de ce dernier, on peut dire que les plus grands diviseurs d'un entier complexe sont cet entier lui-même et ses associés.

Un entier complexe $a+bi$ autre que i^e , est dit composé lorsqu'il peut se décomposer en deux facteurs qui ne sont ni l'un ni l'autre de la forme i^e . Dans le cas contraire il s'appelle premier.

Il est facile de voir que des nombres associés sont toujours simultanément des nombres premiers ou simultanément des nombres composés, et qu'il en est de même pour deux nombres conjugués.

§. 2.

Si m et m_1 désignent deux entiers complexes quelconques, on pourra toujours trouver un entier complexe q tel que l'on ait:

$$N(m - m_1q) = \frac{1}{2}N(m_1).$$

Il suffit, pour s'en assurer, de remarquer qu'on a :

$$N(m - m_1 q) = N(m_1) N\left(\frac{m}{m_1} - q\right),$$

et que les deux entiers réels qui entrent dans q , peuvent toujours être choisis de manière à différer de la partie réelle de $\frac{m}{m_1}$ et du coefficient de i dans cette même expression, de quantités réelles dont les valeurs numériques ne surpassent pas le nombre $\frac{1}{2}$. Il est facile de fonder là-dessus un procédé propre à faire découvrir le plus grand diviseur commun de deux entiers complexes m et m_1 quelconques. On formera les équations :

$$m = m_1 q + m_2, \quad m_1 = m_2 q_1 + m_3, \quad \dots, \quad m_h = m_{h+1} q_h,$$

où les entiers q, q_1, \dots sont choisis de manière que l'on ait :

$$N(m_2) \leq \frac{1}{2} N(m_1), \quad N(m_3) \leq \frac{1}{2} N(m_2), \quad \dots,$$

ce qui aura nécessairement pour effet de conduire à une dernière équation où $m_{h+2} = 0$. Cela fait, il suffit de parcourir les équations précédentes, pour voir que tout diviseur commun de m et m_1 divise aussi les entiers m_2, m_3, \dots, m_{h+1} . Si l'on considère ensuite les mêmes équations en sens inverse, on voit sur le champ que réciproquement tout diviseur de m_{h+1} est aussi diviseur commun de m et m_1 , d'où l'on conclut que le plus grand diviseur commun cherché est l'entier m_{h+1} ou l'un de ses associés, et que dans le cas particulier où m et m_1 sont premiers entre eux, m_{h+1} sera toujours de la forme i^e .

Le procédé précédent conduit à la démonstration du théorème suivant :

„Si, m et m_1 étant premiers entre eux, le produit mn est divisible par m_1 , n sera nécessairement un multiple de m_1 .“

En effet d'après ce qui précède, on aura nécessairement $m_{h+1} = i^e$. D'un autre côté, comme mn est supposé divisible par m_1 , on conclut des équations précédentes multipliées par n , que les produits $m_2 n, m_3 n, \dots, m_{h+1} n$ sont également des multiples de m_1 , conclusions dont la dernière coïncide avec le résultat qu'il s'agit d'établir.

Le théorème que nous venons de démontrer, étant entièrement semblable à celui qui dans la théorie ordinaire sert de base à toutes les recherches sur les nombres en tant qu'ils sont divisibles les uns par les autres, décomposables en facteurs simples etc., on en tirera les mêmes conséquences pour la théorie des nombres complexes.

En considérant en particulier m_1 comme un nombre premier absolu, on en conclut qu'un pareil nombre, pour diviser le produit de deux ou d'un plus grand nombre de facteurs, doit diviser au moins l'un de ces facteurs. De là suit encore qu'un entier premier à plusieurs autres l'est aussi à leur produit, qu'un entier divisible par plusieurs autres qui n'ont pas de diviseur commun, pris deux à deux, l'est de même par le produit de ces derniers, et ainsi de suite.

Le théorème connu d'après lequel un nombre réel ne peut se décomposer que d'une seule manière en facteurs simples réels, a aussi son analogue dans la théorie des nombres complexes. Mais de même que dans le théorème énoncé on considère tacitement les facteurs simples comme positifs ou du moins pris chacun avec un signe déterminé, il faut agir ici d'une manière analogue. Supposons pour cela que dans chaque groupe de nombres associés, on distingue l'un d'entre eux, d'ailleurs arbitrairement choisi, en l'appelant nombre primaire. Dans cette hypothèse, un entier quelconque m pourra toujours se mettre sous la forme:

$$m = i^{\nu} abc \dots$$

a, b, c étant des nombres premiers primaires, égaux ou inégaux, et il est facile de s'assurer que la décomposition précédente est toujours unique. En effet si l'on suppose encore:

$$m = i^{\nu'} a' b' c' \dots$$

a', b', c' étant pareillement des nombres premiers primaires, il faudra nécessairement, pour que ces deux équations s'accordent, que a divise l'un des nombres a', b', c', \dots . Or ces derniers étant premiers et primaires, a devra coïncider avec l'un d'entre eux, avec a' par exemple. Divisant les deux équations par a et continuant de procéder toujours de la même manière, l'identité des deux décompositions se trouvera établie. Si, comme on le fait dans la théorie ordinaire, on réunit les facteurs simples égaux sous forme de puissances, on aura donc d'une manière unique:

$$m = i^{\nu} a^{\alpha} b^{\beta} c^{\gamma} \dots,$$

a, b, c, \dots désignant des nombres premiers primaires inégaux et les exposants α, β, \dots étant tous au moins égaux à l'unité, c'est-à-dire que les bases et leurs exposants, de même que le facteur i^{ν} , seront complètement déterminés dès que le nombre m sera donné.

§. 3.

Avant d'aller plus loin, il convient de rechercher les conditions propres à faire reconnaître si un entier complexe est premier ou composé.

I. Considérons d'abord un nombre binôme $a+bi$, et soit $N(a+bi) = p$. Cela posé, il est facile de prouver que $a+bi$ est un nombre premier ou non suivant que sa norme, considérée au point de vue ordinaire, est elle-même un nombre premier ou composé. Observons d'abord que, si $a+bi$ est composé, en sorte qu'on puisse supposer:

$$a+bi = (c+di)(f+gi), \quad N(c+di) > 1, \quad N(f+gi) > 1,$$

on aura:

$$N(a+bi) = N(c+di)N(f+gi),$$

c'est-à-dire $N(a+bi)$ égal à un nombre composé. Ce premier point établi, il ne reste évidemment qu'à prouver que si $N(a+bi) = a^2 + b^2$ est un nombre composé, $a+bi$ sera aussi composé, pour que la proposition se trouve démontrée. Soit:

$$a^2 + b^2 = mn,$$

m et n étant deux entiers réels l'un et l'autre différents de l'unité. Si maintenant $a+bi$, et par suite aussi $a-bi$, était supposé premier, l'équation précédente mise sous la forme $(a+bi)(a-bi) = mn$, exigerait d'après le théorème démontré à la fin du paragraphe précédent, que m et n fussent également des nombres premiers, sans quoi le second membre renfermerait plus de facteurs simples que le premier, et il faudrait de plus que m , abstraction faite d'un facteur de la forme i^e , coïncidât avec l'un des nombres $a+bi$, $a-bi$, ce qui est impossible, ces derniers étant binômes, tandis que m est monôme.

II. D'après ce qu'on vient de prouver, on voit que pour assigner tous les nombres premiers binômes, tout revient à découvrir quels sont, parmi les nombres premiers réels et positifs, ceux qui peuvent se décomposer en deux carrés. Pour ceux de la forme $4n+3$, une pareille décomposition est impossible, la somme de deux carrés étant toujours de l'une des formes:

$$4n, \quad 4n+1, \quad 4n+2.$$

Il ne reste donc que les nombres premiers $4n+1$ et le nombre 2.

Soit p un nombre premier $4n+1$, il sera facile de prouver, qu'il existe toujours deux groupes de nombres premiers binômes associés ayant p pour norme commune. Cela résulte immédiatement du théorème connu, d'après lequel un nombre premier $4n+1$ est toujours la somme de deux carrés, et ne l'est que d'une seule manière. Mais nous n'avons pas besoin de ce théorème, qui peut être considéré au contraire comme un corollaire de la théorie des nombres complexes. Nous supposerons seulement qu'on sache que l'entier réel ξ peut

toujours être choisi de manière à rendre la formule ξ^2+1 divisible par p , comme cela résulte entr'autres du théorème de WILSON, en vertu duquel on peut poser:

$$\xi = 1.2\dots\frac{1}{2}(p-1).$$

Le produit $(\xi+i)(\xi-i)$ étant ainsi divisible par le nombre p , qui ne divise évidemment ni l'un ni l'autre de ces deux facteurs, on en conclut que p est un nombre composé. Soit en conséquence:

$$p = (a+bi)(c+di), \quad a^2+b^2 > 1, \quad c^2+d^2 > 1.$$

on aura $p^2 = (a^2+b^2)(c^2+d^2)$, d'où l'on conclut, le nombre réel p^2 ne comportant que la seule décomposition $p \times p$ en facteurs positifs différents de l'unité:

$$p = a^2+b^2 = (a+bi)(a-bi),$$

où les deux facteurs évidemment binômes $a+bi$, $a-bi$, dont la norme commune est un nombre premier réel, seront premiers.

Remarquons encore que les nombres premiers $a+bi$ et $a-bi$ sont toujours distincts, c'est-à-dire qu'ils ne sont ni égaux ni associés. En effet, comme a , b sont évidemment l'un pair, l'autre impair, la supposition:

$$a-bi = i^e(a+bi)$$

exigerait d'abord $i^e = \pm 1$, et par suite l'une de celles-ci: $a = 0$, $b = 0$, dont l'impossibilité est manifeste.

On voit donc qu'il existe toujours deux groupes distincts de nombres premiers binômes ayant pour norme commune un nombre premier positif $4n+1$ quelconque, et l'on peut ajouter qu'il n'en existe que deux, car il résulte du théorème déjà cité que, si l'on suppose:

$$(a'+b'i)(a'-b'i) = (a+bi)(a-bi),$$

chacun des facteurs du premier membre est nécessairement égal ou associé à l'un des facteurs du second.

Le nombre 2 qui est également décomposable en deux carrés, ne donne lieu qu'à un seul groupe de nombres premiers binômes, les deux nombres conjugués $1+i$, $1-i$ appartenant pour ce cas au même groupe.

III. Il ne reste qu'à examiner quels sont les nombres monômes qui jouent le rôle de nombres premiers dans la théorie des entiers complexes. Comme sous le rapport dont il s'agit, un nombre quelconque se trouve dans la même catégorie que ses associés, nous n'aurons qu'à considérer des nombres monômes positifs, et comme, parmi ces derniers, ceux qui sont composés au point de vue ordinaire, le sont également dans la théorie des entiers complexes,

il n'est plus question que des nombres premiers positifs. Or, les nombres premiers $4n+1$ et le nombre 2 ayant déjà été reconnus comme nombres composés, il ne reste en définitif qu'à considérer les nombres premiers $4n+3$, par rapport auxquels il est facile de s'assurer qu'ils sont ici des nombres premiers, comme ils le sont au point de vue ordinaire. En effet, si pour un nombre q de cette espèce on avait :

$$q = (a+bi)(c+di). \quad N(a+bi) > 1, \quad N(c+di) > 1,$$

et par suite $q^2 = (a^2+b^2)(c^2+d^2)$, il faudrait, q^2 n'étant susceptible que d'une seule décomposition en facteurs positifs différents de l'unité, qu'on eût $q = a^2+b^2$, ce qui est impossible, comme nous l'avons déjà remarqué.

IV. Les nombres complexes considérés relativement au diviseur $1+i$ et à sa seconde puissance $(1+i)^2 = 2i$, forment trois classes, pour la désignation desquelles il est utile d'introduire des dénominations spéciales.

Un nombre sera dit *impair* lorsqu'il n'est pas divisible par $1+i$. *semi-pair* lorsqu'il est divisible par $1+i$ sans l'être par $(1+i)^2$ ou, ce qui revient au même, par 2, et *pair* enfin lorsqu'il peut être divisé par 2. Il est évident qu'un entier complexe $a+bi$ présentera le premier cas lorsque les deux entiers réels a et b sont l'un pair, l'autre impair, le second lorsque ces deux entiers sont l'un et l'autre impairs, et enfin le troisième lorsque a et b sont tous deux pairs.

V. Nous avons déjà eu occasion de remarquer qu'il peut être utile de distinguer l'un des quatre nombres associés qui forment un même groupe, pour le considérer en quelque sorte comme le nombre primitif ou primaire de ce groupe, les trois autres étant censés dérivés de celui-là en le multipliant par -1 , $\pm i$. Le besoin d'une telle distinction réglée sur un principe invariable, se fera surtout sentir en tant qu'il s'agira de nombres impairs, et nous conviendrons donc de considérer comme le nombre *primaire* dans un groupe d'entiers complexes impairs, celui évidemment unique $a+bi$ pour lequel on a simultanément :

$$a \equiv 1 \pmod{4}, \quad b \equiv 0 \pmod{2}.$$

Il est facile de conclure de cette définition que le produit de deux et par suite d'un nombre quelconque d'entiers impairs primaires, est lui-même un entier primaire.

Cette convention embrasse déjà tous les nombres premiers, à l'exception de ceux qui dérivent du nombre 2, et qui sont $1+i$, $-1+i$, $-1-i$, $1-i$. Quoique, relativement à ces derniers, le choix d'un nombre primaire soit peu utile, nous conviendrons pour plus d'uniformité de regarder comme tel le nombre $1+i$.

§. 4.

Étant donné un entier complexe quelconque m , on peut toujours concevoir la série complète des entiers complexes, distribuée en séries partielles, deux entiers étant rangés dans la même série ou dans des séries distinctes, suivant que leur différence est un multiple de m ou non. Si ensuite on choisit dans chacune de ces séries partielles l'un quelconque des termes qui la composent, on aura ce que nous appellerons *un système de résidus* pour le module donné m . Un pareil système jouit donc de la double propriété de contenir un terme et de n'en contenir qu'un, qui soit congru à un entier quelconque suivant le module auquel il répond. Pour construire un système de résidus, tout se réduit à découvrir quelque condition qui soit satisfaite par l'un des termes de toute série partielle et ne le soit que par ce seul terme, et à assigner ensuite tous les entiers distincts qui remplissent la condition dont il s'agit. On parviendra, par exemple, à une condition de ce genre, si l'on cherche d'abord, $x+yi$ désignant le terme général d'une série partielle donnée, pour quels termes de cette dernière y a la plus petite valeur non-négative, et si l'on choisit ensuite, parmi ces termes en nombre infini, celui nécessairement unique où x , supposé pareillement non-négatif, est à son tour un minimum. Pour découvrir la nature d'un pareil terme, soit $m = a+bi$, et désignons par $\alpha+\beta i$ un entier complexe arbitrairement choisi. On aura alors pour le terme général de la série partielle à laquelle cet entier appartient:

$$x+yi = (a+bi)(t+ui) + \alpha + \beta i, \quad x = at - bu + \alpha, \quad y = bt + au + \beta,$$

où t et u désignent tous les entiers réels depuis $-\infty$ jusqu'à ∞ . On voit, par la dernière de ces équations, que les valeurs dont y est susceptible, sont toutes telles qu'on ait $y \equiv \beta \pmod{h}$, h désignant le plus grand diviseur commun (positif) de a et b . Il résulte de là que y peut toujours être égal à l'un des entiers $0, 1, 2, \dots, h-1$, et ne peut être égal qu'à l'un d'entre eux. Soit donc y_0 celui de ces entiers qui satisfait à la congruence précédente. Pour que y obtienne cette valeur particulière, on aura à satisfaire à l'équation:

$$bt + au = y_0 - \beta,$$

toujours résoluble et dont la solution complète, exprimée en fonction d'une solution particulière t_0, u_0 , est:

$$t = t_0 + \frac{a}{h} z, \quad u = u_0 - \frac{b}{h} z,$$

z désignant un entier réel arbitraire. Au moyen de ces expressions, l'équation en x deviendra:

$$x = at_0 - bu_0 + \frac{p}{h}z,$$

où l'on suppose $a^2 + b^2 = p$. Comme il reste l'indéterminée z dont nous pouvons disposer à volonté, on voit que la plus petite valeur dont x soit susceptible, est l'une de celles-ci:

$$0, 1, 2, \dots, \frac{p}{h} - 1,$$

et il est également manifeste que parmi ces dernières il n'en existe qu'une seule que x puisse comporter. Ayant ainsi reconnu que dans toute série partielle il existe toujours un terme unique pour lequel x et y soient respectivement compris dans les suites:

$$x = 0, 1, 2, \dots, \frac{p}{h} - 1, \quad y = 0, 1, 2, \dots, h - 1,$$

on voit que pour obtenir un système de résidus pour le module $a + bi$, on n'a qu'à introduire, dans l'expression $x + yi$, les valeurs précédentes combinées entre elles de toutes les manières.

Il y a un cas particulier qui mérite une attention particulière; c'est celui où a et b sont premiers entre eux, le système à former se réduisant alors simplement à la suite:

$$0, 1, 2, \dots, p - 1,$$

de sorte que pour un module m de cette nature, on peut toujours satisfaire par un entier réel ξ à la congruence:

$$\xi \equiv k \pmod{m},$$

où k désigne un entier complexe quelconque.

§. 5.

Le résultat auquel nous venons de parvenir, donne lieu à plusieurs conséquences importantes que nous allons rapidement indiquer.

I. On voit d'abord que le système des résidus qui répond à un module quelconque m , contient toujours un nombre de termes exprimé par:

$$N(m),$$

car on a $\frac{p}{h}h = p = N(m)$.

II. On peut encore assigner séparément combien parmi ces termes il y en a de divisibles par un facteur k de m . Il est en effet facile de

voir que ces derniers, étant divisés par k , constitueront un système de résidus pour le module $\frac{m}{k}$, en sorte que le nombre qu'il s'agit d'obtenir, est exprimé par :

$$N\left(\frac{m}{k}\right).$$

III. Connaissant, par ce qui précède, le nombre des termes dont tout système de résidus pour le module m doit se composer, on peut en conclure que si l'on a $N(m)$ entiers tels que la différence de deux quelconques d'entre eux ne soit pas un multiple de m , on est dès lors assuré que ces entiers forment un système de résidus relativement au module m .

Pour faire une application de ce principe, soit μ le terme général d'un système de résidus pour le module m , et désignons par n et l deux entiers déterminés dont le premier n'ait pas de diviseur commun avec m . Cela posé, je dis que l'expression $n\mu + l$ représentera également un pareil système. En effet, les valeurs de cette expression étant en nombre convenable, il ne reste plus qu'à s'assurer que deux quelconques d'entre elles ne sauraient présenter une différence multiple de m . Or cela est évident, puisque, μ' et μ'' désignant deux des valeurs dont μ est susceptible, la différence $n\mu' + l - (n\mu'' + l)$ est égale au produit $n(\mu' - \mu'')$, dont le premier facteur n'a pas de diviseur commun avec m , et dont le second n'est pas un multiple de cet entier.

L'expression $n\mu + l$ représentant un système de résidus, on voit que parmi les valeurs que μ comporte, il y a toujours une valeur unique telle que cette expression soit divisible par m , ou en d'autres termes, que la congruence :

$$nx + l \equiv 0 \pmod{m},$$

lorsque n n'a pas de diviseur commun avec m , est toujours possible, et que sa solution générale est de la forme :

$$x \equiv x_0 \pmod{m},$$

x_0 désignant une solution particulière, de sorte que cette congruence a une racine unique, en considérant à l'ordinaire comme ne constituant qu'une seule racine, toutes les valeurs qui diffèrent les unes des autres de multiples du module. La congruence en question étant équivalente à l'équation :

$$nx + my + l = 0,$$

on voit encore que la solution générale de celle-ci est donnée par les formules :

$$x = x_0 + mz, \quad y = y_0 - nz,$$

x_0, y_0 désignant une solution particulière quelconque, et z étant un entier com-

plexe arbitraire. Quant à la résolution effective de cette équation ou de la congruence équivalente, elle peut s'effectuer au moyen de l'algorithme employé plus haut pour découvrir le plus grand diviseur commun de deux entiers complexes; mais comme nous n'aurons pas à en faire usage, nous ne nous arrêtons pas sur cette résolution, d'ailleurs entièrement semblable à celle qui concerne les entiers réels.

IV. Soient maintenant a, b, c, \dots des entiers complexes en nombre quelconque et premiers entre eux. Construisons des systèmes de résidus pour chacun de ces entiers ainsi que pour leur produit $m = abc\dots$, et désignons par $\alpha, \beta, \gamma, \dots$ et μ les termes généraux de ces systèmes. Cela posé, si relativement à chacun des entiers μ , nous déterminons les nombres $\alpha, \beta, \gamma, \dots$ qui en diffèrent respectivement d'un multiple de a, b, c, \dots , à tout entier μ se trouvera correspondre une combinaison unique de la forme $\alpha, \beta, \gamma, \dots$. Prouvons réciproquement que toute combinaison de cette espèce provient toujours de l'un des entiers μ , et ne saurait provenir que de l'un d'entre eux. Cette dernière assertion est facile à justifier; en effet si la même combinaison répondait à deux entiers μ distincts, leur différence serait divisible par a, b, c, \dots et par suite aussi par m , ce qui est contraire à la nature du système dont μ désigne le terme général. Ayant ainsi reconnu que les combinaisons qui proviennent des entiers μ , sont toutes différentes entre elles, il suffit de remarquer que le nombre de toutes les combinaisons possibles est évidemment:

$$N(a)N(b)N(c)\dots = N(m),$$

c'est-à-dire égal à celui des entiers μ , pour que la proposition énoncée se trouve établie.

V. Il est facile de voir que si μ est premier à m , les entiers correspondants $\alpha, \beta, \gamma, \dots$ seront *tous* respectivement premiers à a, b, c, \dots et réciproquement. Si donc, relativement à un entier quelconque l , on désigne par $\psi(l)$ le nombre de ceux des termes formant un système de résidus pour le module l qui n'ont pas de diviseur commun avec ce dernier, on aura pour un module m décomposé en facteurs a, b, c, \dots premiers entre eux:

$$\psi(m) = \psi(a)\psi(b)\psi(c)\dots$$

VI. Nous pouvons, au moyen de la remarque qui vient d'être faite, déterminer la fonction $\psi(m)$ pour un module m quelconque. Soit d'abord $m = a^\alpha$, a désignant un nombre premier et l'exposant α étant au moins égal

à l'unité. Pour ce cas on obtiendra évidemment le nombre de ceux des termes formant le système des résidus pour le module m qui sont premiers à m , si du nombre total des termes du système on retranche le nombre de ses termes divisibles par a . Ces nombres étant le premier égal à $N(a^a)$ et le second égal à $N(a^{a-1})$ (voyez plus haut I. et II.), on obtiendra pour la différence cherchée:

$$N(a^a) - N(a^{a-1}) = (A-1)A^{a-1},$$

en supposant $A = N(a)$.

Après cela il est facile de voir que relativement à un nombre quelconque:

$$m = i^{\alpha} a^{\alpha} b^{\beta} c^{\gamma} \dots,$$

a, b, c, \dots étant des nombres premiers primaires inégaux et les exposants $\alpha, \beta, \gamma, \dots$ étant tous différents de zéro, on aura:

$$\psi(m) = (A-1)A^{a-1} \cdot (B-1)B^{\beta-1} \cdot (C-1)C^{\gamma-1} \dots$$

en posant pour abrégér:

$$N(a) = A, \quad N(b) = B, \quad N(c) = C, \quad \dots,$$

et l'on doit ajouter que, lorsque m est de la forme i^{α} , la fonction $\psi(m)$ se réduit à l'unité positive.

Théorie des résidus quadratiques.

§. 6.

Étant donnés deux entiers complexes quelconques k et m , le premier est dit *résidu* ou *non-résidu quadratique* par rapport au second, suivant que la congruence:

$$x^2 \equiv k \pmod{m},$$

dont l'inconnue x est aussi considérée comme complexe, est ou n'est pas possible.

Pour procéder du simple au composé, dans la recherche des conditions propres à distinguer l'un de l'autre ces deux cas, nous considérons en premier lieu m comme un nombre premier impair*) non-diviseur de k qui reste quelconque. Soit:

$$(M) \quad \mu_1, \mu_2, \mu_3, \dots$$

le système des résidus relatif au module m , à l'exclusion de celui des termes

*) Le cas où le module se réduit à la forme i^{α} , ne donne lieu à aucune question, un entier quelconque étant toujours résidu quadratique d'un tel module. Il est néanmoins bon d'observer que les formules qu'on va établir, lorsqu'on y suppose m de cette forme, ne donnent rien d'inexact, pour être dispensés dans les recherches générales d'avoir égard à ce cas singulier.

de ce système qui est un multiple de m . Cela étant, la congruence :

$$\mu x \equiv k \pmod{m},$$

où μ désigne l'un quelconque des entiers du système (M) , sera toujours satisfaite par une valeur unique x comprise dans la suite (M) . Distinguons maintenant les deux cas différents que la relation de k à m peut présenter, et supposons d'abord que k soit non-résidu quadratique relativement à m . Dans cette hypothèse, x sera toujours différent de μ , d'où il suit que les entiers (M) peuvent être distribués en groupes composés chacun de deux termes dont le produit soit congru à $k \pmod{m}$. Or, le nombre de ces groupes étant évidemment $\frac{1}{2}(p-1)$, où l'on suppose $p = N(m)$, on aura en multipliant :

$$\mu_1 \mu_2 \mu_3 \dots \equiv k^{\frac{1}{2}(p-1)} \pmod{m}.$$

Dans la seconde hypothèse qui est celle de k résidu quadratique par rapport à m , la distribution en groupes peut encore s'effectuer sur la suite (M) , après en avoir retranché les termes μ tels que $\mu^2 \equiv k \pmod{m}$. Mais comme les termes qui satisfont à cette dernière condition, évidemment toujours au nombre de deux, et tels que l'un est congru à l'autre pris avec le signe moins, donnent un produit congru à $-k \pmod{m}$, on voit qu'en multipliant ce produit par tous les autres termes rangés en groupes, il viendra :

$$\mu_1 \mu_2 \mu_3 \dots \equiv -k^{\frac{1}{2}(p-1)} \pmod{m}.$$

Comme le produit $\mu_1 \mu_2 \mu_3 \dots$ est indépendant de l'entier k , nous pouvons le déterminer en attribuant à k une valeur particulière. Si l'on suppose à cet effet $k = 1$, ce qui se rapporte évidemment au second cas, on trouve le résultat :

$$\mu_1 \mu_2 \mu_3 \dots \equiv -1 \pmod{m},$$

qui est analogue au théorème connu de WILSON et au moyen duquel les congruences précédentes, réunies en une seule, prennent cette forme plus simple :

$$k^{\frac{1}{2}(p-1)} \equiv \pm 1 \pmod{m},$$

où il faut prendre le signe supérieur ou le signe inférieur, suivant que k est ou n'est pas résidu quadratique relativement à m .

Nous conviendrons de désigner désormais par $\left[\frac{k}{m} \right]$ le nombre ± 1 qui entre dans la congruence précédente, de sorte qu'on aura :

$$k^{\frac{1}{2}(p-1)} \equiv \left[\frac{k}{m} \right] \pmod{m}.$$

Le symbole $\left[\frac{k}{m} \right]$ est analogue à celui que LEGENDRE a introduit, et dont l'usage est aujourd'hui généralement adopté; mais il importe de ne pas confondre

ces deux genres de notations dont la seconde, restreinte aux entiers réels, n'exprime pas toujours la même valeur que celle que nous venons de proposer désigne pour ce cas particulier. C'est ce qu'on voit par exemple, en supposant $k = 2$, $m = 3$, puisqu'on a alors :

$$\left[\frac{2}{3}\right] = 1, \quad \left(\frac{2}{3}\right) = -1.$$

Cette circonstance n'a d'ailleurs rien qui puisse étonner, une congruence telle que $x^2 \equiv 2 \pmod{3}$, qui n'est pas possible tant que l'inconnue est supposée réelle, pouvant admettre des solutions, lorsque cette inconnue est considérée comme susceptible de valeurs imaginaires.

Relativement à la notation que nous venons d'adopter, on a les deux équations évidentes :

$$(a) \quad \left[\frac{k}{m}\right] = \left[\frac{l}{m}\right], \quad \left[\frac{k}{m}\right]\left[\frac{k'}{m}\right]\left[\frac{k''}{m}\right] \dots = \left[\frac{kk'k'' \dots}{m}\right],$$

où l'on suppose $k \equiv l \pmod{m}$, et où k, k', k'', \dots sont des entiers quelconques non-divisibles par m .

Nous allons maintenant faire voir que la question de savoir si k est ou n'est pas résidu quadratique par rapport à m , peut toujours se ramener à une question analogue, mais qui ne porte que sur des entiers réels; en d'autres termes, nous démontrerons qu'une expression telle que $\left[\frac{k}{m}\right]$ est toujours réductible à une autre de la forme $\left(\quad\right)$.

Avant de montrer comment cette réduction peut être effectuée, nous remarquerons que, l'expression $\left[\frac{k}{m}\right]$ restant évidemment invariable lorsque le nombre m est remplacé par l'un de ses associés, il sera permis de supposer désormais $m = a + bi$, a et b étant respectivement impair et pair. Cela posé, nous traiterons successivement le cas où $b = 0$ et celui où b est différent de zéro.

1. Dans le premier de ces deux cas, on a $m = a$, a désignant, abstraction faite du signe, un nombre premier réel $4n + 3$. Posons de plus $k = \alpha + \beta i$. Pour obtenir la valeur de $\left[\frac{\alpha + \beta i}{a}\right]$, tout se réduit à voir si la congruence :

$$(1) \quad x^2 \equiv \alpha + \beta i \pmod{a}$$

est ou n'est pas possible. Si l'on y suppose $x = g + \psi i$, cette congruence se décomposera en ces deux congruences simultanées équivalentes qui ne contiennent

que des entiers réels:

$$(2) \quad g^2 - \psi^2 \equiv a, \quad 2g\psi \equiv \beta \pmod{a}.$$

Ces dernières étant élevées au carré et ajoutées donnent:

$$(g^2 + \psi^2)^2 \equiv a^2 + \beta^2 \pmod{a},$$

ou ce qui revient au même, $a^2 + \beta^2$ n'étant pas divisible par a :

$$(3) \quad \left(\frac{a^2 + \beta^2}{a}\right) = 1,$$

de sorte que la possibilité de la congruence (1) suppose la condition (3). Je dis réciproquement que si cette dernière est satisfaite, la possibilité de la congruence (1), ou ce qui revient au même, celle des deux congruences simultanées (2) s'ensuit. Considérons d'abord le cas où $a \equiv 0 \pmod{a}$ et dans lequel la condition (3) a évidemment lieu. On voit qu'on satisfait alors à la première des congruences (2), en posant $\psi = \pm g$, ce qui change la seconde en celle-ci: $2g^2 = \pm \beta^2 \pmod{a}$, évidemment possible si le signe est convenablement choisi. Reste à considérer le cas où a n'est pas divisible par a . En vertu de la condition (3) supposée satisfaite, il existera un entier réel s tel qu'on ait $s^2 \equiv a^2 + \beta^2$, et par suite $(s + \beta)(s - \beta) \equiv a^2 \pmod{a}$. Or, a n'étant pas divisible par a , on conclut de cette dernière congruence:

$$\left(\frac{s + \beta}{a}\right) = \left(\frac{s - \beta}{a}\right) = \pm 1,$$

et nous observerons qu'on peut toujours faire en sorte que le signe supérieur ait lieu. En effet la congruence en s , d'où nous sommes parti, ne contenant que le carré s^2 , nous pouvons, lorsque le signe inférieur a lieu, remplacer s par $-s$, ce qui changera les expressions $\left(\frac{s + \beta}{a}\right)$, $\left(\frac{s - \beta}{a}\right)$ respectivement en $-\left(\frac{s - \beta}{a}\right)$, $-\left(\frac{s + \beta}{a}\right)$. On voit donc que, si s est convenablement choisi, on a:

$$\left(\frac{s + \beta}{a}\right) = \left(\frac{s - \beta}{a}\right) = 1.$$

Cela supposé, on pourra trouver deux entiers réels t et u tels qu'on ait:

$$t^2 \equiv s + \beta, \quad u^2 \equiv s - \beta \pmod{a},$$

et par suite:

$$(tu)^2 \equiv s^2 - \beta^2 \equiv a^2, \quad tu \equiv \pm a \pmod{a},$$

le signe ambigu dépendant du choix de t et u . Ajoutons que, les entiers t et u pouvant être pairs ou impairs à volonté, il sera toujours possible de les

choisir de même espèce, c'est-à-dire tous les deux pairs ou tous les deux impairs. Cela fait, il est facile de voir qu'on satisfera aux congruences (2) au moyen de ces expressions entières:

$$g = \frac{1}{2}(t \pm u), \quad \psi = \frac{1}{2}(t \mp u),$$

où nous supposons que les signes soient choisis conformément à celui qui a lieu dans la congruence $tu \equiv \pm a$. C'est ce dont on s'assure sans difficulté, en faisant la substitution et en ayant égard aux conditions auxquelles s, t, u sont supposés satisfaire.

Il résulte de ce qui précède que si l'on a $\left[\frac{a + \beta i}{a} \right] = 1$, il s'ensuit $\left(\frac{a^2 + \beta^2}{a} \right) = 1$, et que la réciproque a également lieu. On conclut de là et de ce que chacune des expressions précédentes est toujours de la forme ± 1 , que quel que soit l'entier $a + \beta i$ non-divisible par le nombre premier a , on a toujours:

$$(b) \quad \left[\frac{a + \beta i}{a} \right] = \left(\frac{a^2 + \beta^2}{a} \right).$$

On peut remarquer que dans le cas particulier où l'un des entiers a, β s'évanouit, on a:

$$\left[\frac{a + \beta i}{a} \right] = 1.$$

II. Considérons maintenant le cas où la partie imaginaire de $m = a + bi$ n'est pas nulle. Pour décider dans ce cas si la congruence $x^2 \equiv a + \beta i \pmod{m}$ est ou n'est pas possible, nous observerons que d'après ce qui a été prouvé plus haut sur les résidus d'un module $a + bi$, pour lequel a et b sont premiers entre eux, nous pouvons considérer x comme réel. Cela étant, la congruence précédente est équivalente à l'équation:

$$x^2 - a - \beta i = (g + \psi i)(a + bi),$$

où à ces équations simultanées qui ne contiennent que des entiers réels:

$$(4) \quad x^2 - a = ag - b\psi, \quad -\beta = bg + a\psi.$$

En les ajoutant, après les avoir multipliées par a et b , on trouve:

$$(5) \quad ax^2 - aa - b\beta = pq.$$

Observons maintenant que $aa + b\beta$ ne saurait être divisible par p . En effet, si cela était, p diviserait aussi x , ce qui est impossible en vertu de la congruence $x^2 \equiv a + \beta i \pmod{a + bi}$, dont le premier membre est, comme le second, premier à $a + bi$ et par conséquent aussi à p , x étant réel. Cela étant, l'équation (5)

donne :

$$(6) \quad \left(\frac{a}{p}\right) = \left(\frac{a\alpha + b\beta}{p}\right).$$

Je dis maintenant que, cette équation qui est une conséquence très simple de la congruence $x^2 \equiv a + \beta i \pmod{m}$ étant supposée satisfaite, la possibilité de la congruence ou, ce qui revient au même, celle des équations (4) s'ensuit. En effet, la condition (6) entraîne immédiatement l'équation (5), qui, en y substituant pour p sa valeur $a^2 + b^2$, se change en :

$$a(x^2 - a - a\psi) = b(\beta + b\psi).$$

Or, a et b n'ayant pas de diviseur commun, il faut qu'on ait $\beta + b\psi = -a\psi$, ψ étant un entier, et par suite $x^2 - a - a\psi = -b\psi$, équations qui coïncident avec celles dont il s'agit de prouver la possibilité.

L'équation (6) pouvant se mettre sous la forme :

$$\left(\frac{a}{p}\right) \left(\frac{a\alpha + b\beta}{p}\right) = 1,$$

on voit que chacune des deux équations :

$$\left[\frac{a + \beta i}{a + bi}\right] = 1, \quad \left(\frac{a}{p}\right) \left(\frac{a\alpha + b\beta}{p}\right) = 1$$

est toujours une conséquence nécessaire de l'autre. De là et de ce que les expressions qui forment leurs premiers membres, sont toujours de la forme ± 1 , on conclut :

$$\left[\frac{a + \beta i}{a + bi}\right] = \left(\frac{a}{p}\right) \left(\frac{a\alpha + b\beta}{p}\right).$$

Cette dernière égalité peut prendre une forme plus simple, car on a toujours :

$$\left(\frac{a}{p}\right) = 1.$$

En effet, l'équation $a^2 + b^2 = p$ donne sur le champ $\left(\frac{p}{a}\right) = 1$, si l'on fait usage du signe de LEGENDRE étendu, comme l'a proposé M. JACOBI, aux nombres composés¹⁾, et par suite $\left(\frac{a}{p}\right) = 1$, p étant positif et de la forme $4n + 1$.

¹⁾ Les théorèmes qui constituent la théorie des résidus quadratiques, en tant qu'il s'agit de nombres réels, étant généralement connus, nous nous dispenserons d'en rappeler les énoncés, lorsque nous aurons à faire usage de ces théorèmes. Quant à l'usage du signe de LEGENDRE, étendu aux nombres composés, qui est moins connu, on peut sur ce point consulter le compte rendu de l'Académie de Berlin, Oct. 1837, ou le §. 2 du Mémoire déjà cité: „Recherches sur diverses applications de l'Analyse infinitésimale à la Théorie des Nombres.“

²⁾ S. 422 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

Nous avons donc, quel que soit l'entier $a + \beta i$ non-divisible par le nombre premier $a + bi$, dans lequel b est pair, mais différent de zéro :

$$(c) \quad \left[\frac{a + \beta i}{a + bi} \right] = \left(\frac{a\alpha + b\beta}{p} \right).$$

Il importe de remarquer que l'équation (b) est tout-à-fait distincte de celle que nous venons d'établir, et ne se déduit nullement de cette dernière, en y faisant $b = 0$.

§. 7.

Nous pouvons maintenant nous occuper de la question que l'on doit regarder comme la plus importante parmi celles que la théorie des résidus quadratiques présente, et qui a pour objet, étant donné un entier complexe quelconque k , d'assigner les caractères propres à distinguer les nombres premiers impairs m dont k est résidu quadratique, de ceux auxquels cet entier a la relation opposée. Comme d'après l'équation (a), démontrée plus haut, la question proposée, lorsque k est un nombre composé, se réduit sur-le-champ à des questions analogues relatives aux facteurs de k , on voit que nous n'aurons à considérer que les quatre hypothèses :

$$k = \pm 1, \quad i, \quad 1+i, \quad a+\beta i,$$

$a + \beta i$ étant un nombre premier impair que nous pourrions considérer comme primaire, mais dans lequel nous supposons simplement que β , qui peut d'ailleurs s'évanouir, est pair.

Le premier cas ne donne lieu à aucune question, ± 1 étant un carré. Les trois autres sont résolus par les équations qui suivent et dans lesquelles le nombre premier impair $a + bi$ est pareillement tel que b , qui peut d'ailleurs se réduire à zéro, soit pair, et où l'on a posé pour abrégé, $a^2 + b^2 = p$:

$$(d) \quad \left[\frac{i}{a + bi} \right] = (-1)^{\frac{1}{2}(p-1)}, \quad \left[\frac{1+i}{a + bi} \right] = (-1)^{\frac{1}{2}((a+b)^2-1)}, \quad \left[\frac{a+\beta i}{a + bi} \right] = \left[\frac{a + \beta i}{a + \beta i} \right].$$

La première de ces équations se déduit sans difficulté, soit de la formule $k^{\frac{1}{2}(p-1)} \equiv \left[\frac{k}{m} \right] \pmod{m}$ obtenue plus haut, soit des deux équations (b) et (c), si, en suivant cette dernière voie, on suppose successivement $b = 0$ et b différent de zéro.

Pour démontrer la seconde des équations (d), soit d'abord $b = 0$. On a alors, au moyen de l'équation (b) et d'un théorème connu:

$$\left[\frac{1+i}{a} \right] = \left(\frac{2}{a} \right) = (-1)^{\frac{1}{2}(a^2-1)},$$

conformément à l'équation qu'il s'agit d'établir. Supposons, en second lieu, b différent de zéro. L'équation (c) donne alors:

$$\left[\frac{1+i}{a+bi} \right] = \left(\frac{a+b}{p} \right).$$

Pour obtenir la valeur du second membre, nous aurons recours à l'équation identique $2p = (a+b)^2 + (a-b)^2$, de laquelle on conclut successivement au moyen de théorèmes connus:

$$\left(\frac{p}{a+b} \right) = \left(\frac{2}{a+b} \right), \quad \left(\frac{a+b}{p} \right) = \left(\frac{2}{a+b} \right) = (-1)^{\frac{1}{2}((a+b)^2-1)},$$

ce qui s'accorde également avec l'équation que nous nous proposons de vérifier.

La démonstration de la troisième des équations (d), à laquelle nous arrivons maintenant et qui exprime une loi de réciprocité entre deux nombres premiers impairs différents, c'est-à-dire ni égaux ni opposés, donne lieu à distinguer trois cas. Le premier de ces cas est celui où b et β sont tous les deux égaux à zéro. Dans ce premier cas, la vérité de l'équation est évidente, puisque d'après la formule (b) on a à la fois:

$$\left[\frac{\alpha}{a} \right] = 1, \quad \left[\frac{a}{\alpha} \right] = 1.$$

Considérons, en second lieu, le cas où l'un des entiers b et β se réduit à zéro, et soit β cet entier évanouissant, ce que la forme symétrique de notre équation permet évidemment de supposer. On a alors, en vertu des équations (c) et (b) et d'après une remarque déjà faite*):

$$\left[\frac{\alpha}{a+bi} \right] = \left(\frac{\alpha\alpha}{p} \right) = \left(\frac{\alpha}{p} \right), \quad \left[\frac{a+bi}{\alpha} \right] = \left(\frac{p}{\alpha} \right),$$

de sorte que la vérification à effectuer résulte de l'équation connue:

$$\left(\frac{\alpha}{p} \right) = \left(\frac{p}{\alpha} \right).$$

Passant enfin au troisième cas où b et β sont l'un et l'autre différents de zéro, on appliquera la formule (c) à chacun des deux membres de l'équation qu'il

*) S. 555: $\left(\frac{\alpha}{p} \right) = 1$. K.

s'agit de prouver et qui deviendra ainsi:

$$\left(\frac{a\alpha + b\beta}{p}\right) = \left(\frac{a\alpha + b\beta}{\bar{\sigma}}\right),$$

en posant, pour un instant, $\alpha^2 + \beta^2 = \bar{\omega}$. Pour s'assurer de la vérité de cette dernière équation, il suffit de recourir à l'identité:

$$(a\alpha + b\beta)^2 + (b\alpha - a\beta)^2 = p\bar{\omega},$$

d'où résulte successivement, $a\alpha + b\beta$ étant impair:

$$\left(\frac{p}{a\alpha + b\beta}\right) = \left(\frac{\bar{\sigma}}{a\alpha + b\beta}\right) \cdot \left(\frac{a\alpha + b\beta}{p}\right) = \left(\frac{a\alpha + b\beta}{\bar{\sigma}}\right), \quad \text{c. q. f. d.}$$

Nous ne terminerons pas ce paragraphe sans observer que les équations (d) sont dues à M. GAUSS qui les a données sans démonstration, du moins la dernière, dans le Mémoire cité plus haut. La démonstration que nous venons de développer, déjà indiquée dans une Note insérée dans le Journal de CRELLE¹⁾, est comme on voit, une application très simple des théorèmes (b) et (c), qui indépendamment de l'usage que nous en faisons ici, nous seront indispensables pour la solution de la question qui fait le principal sujet du présent Mémoire.

§. 8.

Le symbole $\left[\frac{k}{m}\right]$, tel que nous l'avons employé jusqu'à présent, suppose que m est un nombre premier impair. Il arrive souvent qu'on a à considérer des produits de la forme:

$$\left[\frac{k}{m}\right]\left[\frac{k}{m'}\right]\left[\frac{k}{m''}\right]\dots,$$

où m, m', m'', \dots sont des nombres premiers impairs non-diviseurs de k , mais d'ailleurs égaux ou inégaux. Soit $M = mm'm''\dots$ et convenons de désigner désormais le produit précédent simplement par:

$$\left[\frac{k}{M}\right],$$

de sorte que la valeur de notre symbole ainsi généralisé, toujours égale soit à $+1$ soit à -1 , n'indiquera plus, suivant ces deux cas, si k est ou n'est pas résidu quadratique par rapport à M , et fera seulement connaître, si parmi les facteurs simples égaux ou inégaux de M , il y en a un nombre pair ou impair,

¹⁾ S. 173 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

auxquels k présente la dernière de ces deux relations. L'extension que nous venons d'indiquer, entièrement semblable à celle que M. JACOBI a proposée relativement au signe de LEGENDRE et dont nous avons déjà fait un fréquent usage dans ce qui précède, donne lieu à plusieurs théorèmes analogues à ceux qui ont été démontrés dans le paragraphe précédent et faciles à déduire de ces derniers. On a d'abord évidemment les équations:

$$(e) \quad \left[\frac{k}{M} \right] = \left[\frac{l}{M} \right], \quad \left[\frac{kk'}{M} \right] = \left[\frac{k}{M} \right] \left[\frac{k'}{M} \right], \quad \left[\frac{k}{MM'} \right] = \left[\frac{k}{M} \right] \left[\frac{k}{M'} \right],$$

qui supposent, la première, que k , toujours sans diviseur commun avec l'entier impair M , est tel qu'on ait $k \equiv l \pmod{M}$, la seconde que k et k' sont premiers à M , et la troisième que k est premier aux entiers impairs M et M' .

Voici maintenant les équations analogues aux équations (d), ou pour mieux dire, d'une forme tout identique avec ces dernières:

$$(f) \quad \left[\frac{i}{A+Bi} \right] = (-1)^{\frac{1}{4}(p-1)}, \quad \left[\frac{1+i}{A+Bi} \right] = (-1)^{\frac{1}{4}(A+B^2-1)}, \quad \left[\frac{\alpha+\beta i}{A+Bi} \right] = \left[\frac{A+Bi}{\alpha+\beta i} \right].$$

Dans ces équations $A+Bi$ et $\alpha+\beta i$ sont deux entiers complexes impairs quelconques premiers entre eux et pour lesquels les coefficients B et β , toujours considérés comme pairs, peuvent se réduire à zéro. On a d'ailleurs $P = A^2 + B^2$.

La première de ces équations coïncidant avec la première des équations (d) déjà établies, lorsque $A+Bi$ se réduit au nombre premier $a+bi$, on voit que pour s'assurer qu'elle a généralement lieu, tout se réduit à faire voir que, si on la suppose exacte pour un nombre quelconque $A+Bi$, elle ne cessera pas de subsister lorsque ce dernier vient à être remplacé par le produit:

$$(a+bi)(A+Bi)$$

que nous désignerons par $A'+B'i$. Nous avons donc à montrer que la troisième des équations:

$$\left[\frac{i}{a+bi} \right] = (-1)^{\frac{1}{4}(p-1)}, \quad \left[\frac{i}{A+Bi} \right] = (-1)^{\frac{1}{4}(P-1)}, \quad \left[\frac{i}{A'+B'i} \right] = (-1)^{\frac{1}{4}(P'-1)},$$

où l'on suppose $p = a^2 + b^2$, $P = A^2 + B^2$, est une conséquence des deux premières. Il suffit évidemment pour cela de prouver que les deux entiers réels:

$$\frac{1}{4}(p-1) + \frac{1}{4}(P-1), \quad \frac{1}{4}(P'-1)$$

sont toujours de même espèce, c'est-à-dire tous les deux pairs ou tous les deux impairs. C'est ce qui résulte sur-le-champ de l'équation identique:

$$\frac{1}{4}(Pp-1) - \frac{1}{4}(p-1) - \frac{1}{4}(P-1) = \frac{1}{4}(P'-1)(p-1)$$

dont le second membre est pair et même divisible par 4, P et p étant de la forme $4n+1$.

Le même moyen de démonstration peut s'appliquer à la seconde des équations (f), et l'on voit qu'il s'agira ainsi de démontrer que les deux nombres:

$$\frac{1}{8}((a+b)^2-1)+\frac{1}{8}((A+B)^2-1), \quad \frac{1}{8}((A'+B')^2-1)$$

sont toujours de même espèce. Observons pour cela qu'en vertu de l'équation identique:

$$\frac{1}{8}(rs)^2-1-\frac{1}{8}(r^2-1)-\frac{1}{8}(s^2-1) = \frac{1}{8}(r^2-1)(s^2-1),$$

dont le second membre est pair, si r et s sont des entiers impairs, le premier des deux entiers que nous avons à considérer, est de même espèce que $\frac{1}{8}[(a+b)(A+B)^2-1]$. Mais, comme d'un autre côté deux carrés dont les racines diffèrent d'un multiple de 8, diffèrent eux-mêmes d'un multiple de 16, ce dernier est à son tour de même espèce que:

$$\frac{1}{8}[(a+b)(A+B)-2Bb]^2-1 = \frac{1}{8}[(A'+B')^2-1],$$

et l'assertion avancée se trouve établie.

La troisième des équations (f) est également très facile à obtenir. En effet, d'après l'hypothèse faite sur les entiers $A+Bi$, $\alpha+\beta i$, on peut les décomposer l'un et l'autre en facteurs simples ayant leurs parties réelles impaires. Soit n l'un des facteurs de $A+Bi$, et m l'un de ceux de $\alpha+\beta i$, on pourra, par l'emploi répété des deux dernières des équations (e), remplacer l'expression $\left[\frac{\alpha+\beta i}{A+Bi}\right]$ par un produit d'expressions de la forme $\left[\frac{m}{n}\right]$, où tout facteur m doit être combiné avec tout facteur n . Si maintenant on remplace tout symbole $\left[\frac{m}{n}\right]$ par celui-ci: $\left[\frac{n}{m}\right]$ qui lui est équivalent en vertu de la troisième des équations (d), et que l'on effectue la multiplication au moyen des équations déjà citées, le premier membre de l'équation qu'il s'agit de vérifier, se trouvera identique au second.

Il reste à opérer d'une manière générale la réduction qui pour le cas particulier d'un nombre premier $a+bi$, peut s'obtenir au moyen des équations (b) et (c) du paragraphe précédent. Soit $A+Bi$ un entier impair quelconque (B étant pair et pouvant se réduire à zéro) et $\alpha+\beta i$ un second entier, assujéti à la condition unique d'être premier à $A+Bi$; il s'agira de remplacer l'expression $\left[\frac{\alpha+\beta i}{A+Bi}\right]$ par des expressions analogues ne contenant que des entiers réels.

Considérons d'abord le cas où B s'évanouit, et celui où A et B n'ont pas de diviseur commun; nous verrons ensuite que le cas le plus général se réduit immédiatement à ceux-là. Relativement aux deux cas qui viennent d'être indiqués, on a respectivement:

$$(g) \quad \left[\frac{\alpha + \beta i}{A} \right] = \left(\frac{\alpha^2 + \beta^2}{A} \right), \quad \left[\frac{\alpha + \beta i}{A + Bi} \right] = \left(\frac{A\alpha + B\beta}{P} \right).$$

P désignant pour abrégé, dans la seconde de ces équations, le binôme $A^2 + B^2$.

Pour démontrer la première, observons qu'on peut y considérer A comme positif, les deux membres ne changeant pas lorsqu'on y remplace A par $-A$. Cela posé, soit:

$$A = aa' \dots \times pp' \dots$$

$a, a', \dots, p, p', \dots$ désignant des nombres premiers réels et positifs, les premiers, a, a', \dots , de la forme $4n + 3$, les seconds, p, p', \dots , de la forme $4n + 1$. D'après l'équation (b), chacun des premiers donne une équation telle que:

$$\left[\frac{\alpha + \beta i}{a} \right] = \left(\frac{\alpha^2 + \beta^2}{a} \right),$$

tandis que pour chacun des derniers, p par exemple, qui peut se décomposer en deux facteurs premiers binômes $(a + bi)(a - bi)$, où b est supposé pair, on a en vertu de l'équation (c):

$$\left[\frac{\alpha + \beta i}{p} \right] = \left[\frac{\alpha + \beta i}{a + bi} \right] \left[\frac{\alpha + \beta i}{a - bi} \right] = \left(\frac{a\alpha + b\beta}{p} \right) \left(\frac{a\alpha - b\beta}{p} \right) = \left(\frac{a^2\alpha^2 - b^2\beta^2}{p} \right),$$

et par suite, puisque $-b^2 \equiv a^2 \pmod{p}$:

$$\left[\frac{\alpha + \beta i}{p} \right] = \left(\frac{a^2}{p} \right) \left(\frac{\alpha^2 + \beta^2}{p} \right) = \left(\frac{\alpha^2 + \beta^2}{p} \right).$$

Ces deux systèmes de relations étant multipliés entre eux, donnent la formule qu'il s'agissait d'établir.

Passons à la vérification de la seconde des équations précédentes (g).

Nous supposons d'abord $\beta = 0$, cas auquel celui où β n'est pas zéro, se ramène facilement. Comme, par hypothèse, A et B n'ont pas de diviseur commun, on pourra poser:

$$A + Bi = (a + bi)(a' + b'i) \dots,$$

où les facteurs du second membre désignent des nombres premiers binômes, dans lesquels b, b', \dots sont supposés pairs. L'équation (c) donne relativement au facteur $a + bi$:

$$\left[\frac{a}{a + bi} \right] = \left(\frac{aa}{p} \right) = \left(\frac{a}{p} \right),$$

en posant pour abrégier $a^2 + b^2 = p$. En faisant le produit de cette équation et des équations analogues, il viendra :

$$\left[\frac{a}{A+Bi} \right] = \left(\frac{a}{pp' \dots} \right) = \left(\frac{a}{P} \right).$$

Or, l'équation qu'il s'agit de prouver se réduisant, par la supposition $\beta = 0$, à celle-ci :

$$\left[\frac{a}{A+Bi} \right] = \left(\frac{Aa}{P} \right) = \left(\frac{A}{P} \right) \left(\frac{a}{P} \right),$$

nous n'avons plus qu'à démontrer qu'on a $\left(\frac{A}{P} \right) = 1$. Mais, comme A et B sont premiers entre eux, il résulte de l'équation $A^2 + B^2 = P$ que A et P sont pareillement sans diviseur commun, de sorte que $\left(\frac{P}{A} \right) = 1$, et par suite $\left(\frac{A}{P} \right) = 1$.

Reste à considérer le cas où β a une valeur différente de zéro. On cherchera alors un entier réel s tel qu'on ait :

$$s \equiv a + \beta i \pmod{A+Bi},$$

dont l'existence suit de l'hypothèse admise sur les nombres A et B . Cela fait, on aura :

$$\left[\frac{a + \beta i}{A+Bi} \right] = \left[\frac{s}{A+Bi} \right]$$

et par suite, en vertu du cas déjà démontré :

$$\left[\frac{a + \beta i}{A+Bi} \right] = \left(\frac{As}{P} \right).$$

D'un autre côté, si l'on remplace la congruence précédente par deux équations équivalentes, on reconnaît sur-le-champ que s satisfait à la condition :

$$As \equiv Aa + B\beta \pmod{P}.$$

Cela étant, cette dernière congruence conduit à l'équation :

$$\left(\frac{As}{P} \right) = \left(\frac{Aa + B\beta}{P} \right),$$

dont la comparaison avec celle que nous avons obtenue plus haut, donne un résultat qui s'accorde avec la seconde des formules (g).

Il nous reste enfin à supposer l'entier impair $A+Bi$ tout-à-fait arbitraire, si ce n'est que nous considérons toujours B comme pair, ce qui ne nuit en

rien à la généralité. Soit L le plus grand diviseur commun (réel) de A et B , et posons :

$$A = A'L, \quad B = B'L, \quad A'^2 + B'^2 = P'.$$

L'expression $\left[\frac{\alpha + \beta i}{A + Bi} \right]$ dans laquelle $\alpha + \beta i$ n'est assujéti qu'à la seule condition d'être premier à $A + Bi$, se décomposera alors en deux facteurs :

$$\left[\frac{\alpha + \beta i}{L} \right], \quad \left[\frac{\alpha + \beta i}{A' + B'i} \right]$$

respectivement de même forme que les premiers membres des équations (g), et l'on aura en conséquence :

$$(h) \quad \left[\frac{\alpha + \beta i}{A + Bi} \right] = \left(\frac{\alpha^2 + \beta^2}{L} \right) \left(\frac{A'\alpha + B'\beta}{P'} \right).$$

§. 9.

Nous terminerons ce que nous avons à dire sur les résidus quadratiques, en considérant la congruence :

$$(1) \quad x^2 \equiv k \pmod{m},$$

où k et m sont des entiers complexes quelconques premiers entre eux, le second impair. Pour que cette congruence soit possible, il faut évidemment qu'elle puisse subsister par rapport à chacun des facteurs simples de m . Soient :

$$j, j', j'', \dots$$

les nombres premiers primaires inégaux qui divisent m et soit μ leur nombre. Il faudra donc qu'on ait :

$$(2) \quad \left[\frac{k}{j} \right] = 1, \quad \left[\frac{k}{j'} \right] = 1, \quad \left[\frac{k}{j''} \right] = 1, \dots$$

Je dis de plus que, ces conditions ayant lieu, la possibilité de la congruence s'ensuit et que le nombre de ses racines sera 2^μ , en considérant à l'ordinaire comme ne constituant qu'une seule racine, les entiers en nombre infini qui diffèrent les uns des autres de multiples du module m . Considérons d'abord la congruence $x^2 \equiv k \pmod{j^n}$, l'exposant étant un nombre positif quelconque. Si l'on y satisfait par la supposition de $x = a$, et par suite par l'hypothèse plus générale de $x = a + tj^h$, t étant un entier arbitraire, il est facile d'en déduire une solution pour la congruence de même forme, mais relative au module

f^{n+l} où l'on suppose $l \leq h$. En effet, la substitution de l'expression de x donnant :

$$\frac{x^2 - k}{f^h} = \frac{a^2 - k}{f^h} + 2at + t^2 f^h,$$

où le premier terme du second membre est par hypothèse un entier, on voit que pour satisfaire à la congruence $x^2 \equiv k \pmod{f^{n+l}}$, il reste à faire en sorte qu'on ait $2at \equiv -\frac{a^2 - k}{f^h} \pmod{f^n}$, ce qui est toujours possible, a et par suite $2a$ étant évidemment premier au module. Comme on peut, par ce procédé, s'élever à des exposants de plus en plus grands, en partant de l'exposant $h = 1$, on voit que la condition de possibilité de la congruence :

$$x^2 \equiv k \pmod{f^h},$$

quel que soit h , est celle qui se rapporte à $h = 1$, consistant en ce que l'on doit avoir :

$$\left[\frac{k}{f} \right] = 1.$$

Voyons maintenant quel est le nombre des racines de la congruence précédente. En considérant toujours a comme une de ses racines, on pourra lui donner la forme :

$$x^2 - a^2 = (x+a)(x-a) \equiv 0 \pmod{f^h}.$$

Or, $x+a$ et $x-a$ ne pouvant être simultanément divisibles par f , on voit qu'on ne peut satisfaire à cette dernière qu'en supposant :

$$x \equiv a \quad \text{ou} \quad x \equiv -a \pmod{f^h},$$

ce qui ne donne que deux racines, qui seront toujours distinctes, leur différence $2a$ n'étant pas divisible par f .

Si maintenant l'on observe qu'en posant $m = i^e f^h f^{h'}$. . . , la congruence (1) est évidemment équivalente à ces congruences simultanées :

$$x^2 \equiv k \pmod{f^h}, \quad x^2 \equiv k \pmod{f^{h'}}, \quad \dots,$$

dont chacune, en vertu de ce qui précède, admet deux racines distinctes de la forme $\pm a$, on conclura facilement, d'après la remarque faite plus haut (§. 5, IV.) que la congruence (1) admet elle-même 2^u racines distinctes, lorsque les conditions (2), nécessaires pour sa possibilité, sont toutes remplies. Il est bon d'ajouter que dans le cas où m est de la forme i^e , et où il n'y a aucune condition à remplir, le nombre des solutions de la congruence (1) est toujours exprimé par la formule 2^u , car on a dans ce cas $\mu = 0$.

Théorèmes fondamentaux sur les formes quadratiques.

§. 10.

Avant d'entrer dans le sujet indiqué par le titre, il convient de faire une remarque nécessaire pour que l'exposition qu'on va lire, soit considérée sous son véritable point de vue. L'objet du présent Mémoire étant purement théorique, nous avons cherché à résoudre les questions que nous avons à traiter, par les considérations qui, théoriquement parlant, nous ont paru les plus simples, sans nous attacher à rendre les solutions propres au calcul numérique. Pour satisfaire à cette dernière condition, il faudrait entrer dans des développements assez étendus, qui ne présenteraient que très peu d'intérêt et ne seraient d'ailleurs d'aucune utilité pour l'objet de pure théorie que nous avons en vue. Limités comme nous venons de l'indiquer, les éléments de la théorie des formes quadratiques à coefficients et à indéterminées complexes peuvent être présentés dans un petit nombre de pages, si aux moyens déjà employés par les illustres géomètres qui ont fondé ou perfectionné la théorie analogue relative aux entiers réels, on ajoute quelques principes nouveaux, qui nous paraissent mériter l'attention des géomètres. Leur extrême fécondité ne sera toutefois mise dans tout son jour que par des recherches ultérieures que nous avons entreprises sur les formes des degrés supérieurs et que nous aurons à exposer plus tard.

Toute expression:

$$(1) \quad ax^2 + 2bxy + cy^2,$$

où a, b, c sont des entiers complexes déterminés, et x, y de pareils entiers indéterminés, est ce que nous appellerons une *forme quadratique binaire* ou simplement une *forme*, cette abréviation ne pouvant donner lieu ici à aucune ambiguïté. Il est essentiel de suivre un ordre fixe tant par rapport aux indéterminées x et y , qui seront respectivement nommées la première et la seconde, que par rapport aux coefficients a, b, c , dont la désignation indiquera toujours la place que ces coefficients occupent dans l'expression que nous venons d'écrire.

Les propriétés de la forme (1) dépendant principalement du nombre D , donné par l'équation $D = b^2 - ac$, ce nombre sera dit le *déterminant* de la forme en question. Dans le cas particulier où D est un carré, ce qui comprend la supposition de $D = 0$, la forme se décompose évidemment en deux facteurs

linéaires à coefficients rationnels, en sorte que ses propriétés se déduisent facilement de celles bien connues des expressions de ce genre. C'est pourquoi nous ferons toujours abstraction de ce cas particulier. Sous cette restriction, les coefficients extrêmes a et c sont l'un et l'autre différents de zéro, d'où il suit que l'un d'entre eux, c par exemple, peut se déduire sans indétermination de l'autre a , du coefficient moyen b et du déterminant D , supposés connus, au moyen de la formule:

$$c = \frac{b^2 - D}{a}.$$

Si dans la forme (1) on remplace les indéterminées x et y par de nouvelles indéterminées x' et y' , liées aux premières par les équations:

$$(2) \quad x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y',$$

où $\alpha, \beta, \gamma, \delta$ sont des entiers donnés, elle se changera en cette autre:

$$(3) \quad a' x'^2 + 2b' x' y' + c' y'^2,$$

où l'on a:

$$(4) \quad a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2, \quad b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta, \quad c' = a\beta^2 + 2b\beta\delta + c\delta^2,$$

et l'on dit alors que la nouvelle forme (3) est *contenue* sous la forme primitive (1). En substituant les coefficients a', b', c' de la forme (3) dans l'expression de son déterminant D' , il viendra:

$$(5) \quad D' = (\alpha\delta - \beta\gamma)^2 D.$$

On voit ainsi qu'une forme contenue sous une autre a toujours un déterminant multiple de celui de cette dernière, et que le quotient de ces déterminants est un carré, d'où il suit que, pour que deux formes puissent se contenir mutuellement, il faut nécessairement que leurs déterminants soient ou égaux ou opposés.

Réciproquement, si les déterminants de deux formes telles que (1) et (3) sont égaux ou opposés, et qu'en outre la première contienne la seconde, je dis que celle-ci contiendra la première. Pour le prouver, remarquons que l'hypothèse $D' = \pm D$, comparée à l'équation (5), donne celle-ci:

$$(6) \quad \alpha\delta - \beta\gamma = \pm 1,$$

les déterminants égaux à zéro étant toujours exclus. Si maintenant l'on résout les équations (2) par rapport à x' et y' , on obtiendra les expressions:

$$(7) \quad x' = \frac{\delta}{\pm 1} x - \frac{\beta}{\pm 1} y, \quad y' = -\frac{\gamma}{\pm 1} x + \frac{\alpha}{\pm 1} y,$$

dont les quatre coefficients sont entiers, et qui, étant introduites dans la forme (3), la feront évidemment coïncider avec la forme (1), ce qu'il s'agissait de prouver.

Deux formes dont chacune contient l'autre, sont dites *équivalentes*. Quoique la relation mutuelle de deux formes, exprimée par cette désignation, puisse subsister aussi bien entre deux formes à déterminants opposés qu'entre deux formes dont les déterminants sont égaux, nous nous bornerons à considérer le dernier de ces deux cas. Il est en effet facile de voir que ces deux cas ne sont pas essentiellement différents, puisque, étant données deux formes qui répondent au premier, il suffit évidemment de multiplier les trois coefficients de l'une d'entre elles respectivement par 1, i , -1 , pour que le groupe des deux formes rentre dans le second de ces deux cas.

La définition de l'équivalence ainsi restreinte, donne encore lieu à une nouvelle subdivision qu'il est essentiel de prendre en considération. Comme on a $D' = D$, et par suite en vertu de l'équation (5):

$$(8) \quad \alpha\delta - \beta\gamma = \pm 1 = \varepsilon,$$

nous pouvons avoir égard au signe dont l'unité est précédée dans cette équation. Nous dirons désormais que la substitution donnée par les formules (2), et qui change la forme (1) dans la forme équivalente (3), est *propre* ou *impropre*, suivant que le signe supérieur ou le signe inférieur a lieu dans l'équation (8). Observons d'abord que la substitution inverse (7) qui sert à revenir de la forme (3) à la forme (1) et qui, pour le cas qui nous occupe, se réduit à poser:

$$x' = \frac{\delta}{\varepsilon}x - \frac{\beta}{\varepsilon}y, \quad y' = -\frac{\gamma}{\varepsilon}x + \frac{\alpha}{\varepsilon}y.$$

sera toujours de même nom que la substitution directe (2). Il suffit, pour s'en assurer, de remplacer dans l'expression (8) les entiers α , β , γ , δ respectivement par $\frac{\delta}{\varepsilon}$, $-\frac{\beta}{\varepsilon}$, $-\frac{\gamma}{\varepsilon}$, $\frac{\alpha}{\varepsilon}$, ce qui changera cette expression en:

$$\frac{\alpha\delta - \beta\gamma}{\varepsilon^2} = \varepsilon.$$

Les deux substitutions étant de même nature quant à la distinction que nous venons de faire, on peut transporter la dénomination précédente au groupe des deux formes et appeler l'équivalence de ces formes propre ou impropre suivant que la valeur de ε , commune aux deux substitutions en question, est

+1 ou -1. Il n'est pas nécessaire pour notre objet de considérer l'équivalence impropre qui au reste se change toujours en équivalence propre, si dans l'une des formes on change le signe du coefficient moyen. En disant donc désormais que deux formes sont équivalentes, nous entendrons toujours qu'il s'agit de l'équivalence propre, ou autrement dit, qu'on peut passer de chacune de ces formes à l'autre, par une substitution telle que (2), où l'on a $\alpha\delta - \beta\gamma = 1$. Pareillement, quand nous nous proposerons de découvrir toutes les transformations qui changent ces formes l'une dans l'autre, nous n'aurons en vue que celles qui satisfont à la condition précédente, et nous rejeterons toutes les transformations pour lesquelles on aurait $\alpha\delta - \beta\gamma = -1$. Comme dans ce qui va suivre, il sera le plus souvent inutile de désigner les indéterminées par des lettres particulières, nous conviendrons d'indiquer une forme telle que (1), ou une substitution telle que (2), par ces notations abrégées:

$$(a, b, c). \quad \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}.$$

La notion de l'équivalence ainsi que nous venons de la fixer, donne lieu à ces théorèmes très simples:

I. Toute forme est équivalente à elle-même, puisqu'il est évident qu'elle ne varie pas, si on lui applique la substitution $\begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}$.

II. Deux formes qui équivalent à une troisième, sont équivalentes entre elles. En effet, si la forme f , supposée équivalente à f' , se transforme en celle-ci au moyen de la substitution $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$, et si f' devient à son tour identique avec f'' , au moyen de la substitution $\begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix}$, on passera évidemment de f à f'' , en faisant usage de la substitution unique $\begin{pmatrix} \alpha'', & \beta'' \\ \gamma'', & \delta'' \end{pmatrix}$, où l'on a:

$$\begin{aligned} \alpha'' &= \alpha\alpha' + \beta\gamma', & \beta'' &= \alpha\beta' + \beta\delta', \\ \gamma'' &= \gamma\alpha' + \delta\gamma', & \delta'' &= \gamma\beta' + \delta\delta', \end{aligned}$$

et il ne reste plus qu'à prouver qu'on a $\alpha''\delta'' - \beta''\gamma'' = 1$. Mais cette équation résulte sur-le-champ de l'équation identique:

$$\alpha''\delta'' - \beta''\gamma'' = (\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma').$$

où l'on a par hypothèse, $\alpha\delta - \beta\gamma = 1$ et $\alpha'\delta' - \beta'\gamma' = 1$.

La substitution $\begin{pmatrix} \alpha'' & \beta'' \\ \gamma'' & \delta'' \end{pmatrix}$, qui produit le même effet que les deux substitutions $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $\begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$, employées l'une après l'autre, peut s'appeler convenablement une *substitution composée*, où il importe de remarquer que l'ordre des substitutions composantes ne peut pas être interverti.

III. Deux formes (a, b, c) et (a', b', c') étant supposées équivalentes, le plus grand diviseur commun des entiers a, b, c est le même que celui des entiers a', b', c' , et la même égalité subsiste entre les deux groupes $a, 2b, c$ et $a', 2b', c'$.

En effet l'équivalence admise supposant une transformation telle que (2), et par suite les équations (4), on voit immédiatement que tout diviseur commun de a, b, c divise aussi a', b', c' , et l'on arrive à un résultat semblable relativement aux groupes $a, 2b, c$ et $a', 2b', c'$, si préalablement on suppose les deux membres de la seconde des équations (4) multipliés par 2. Un raisonnement analogue pouvant se faire en sens inverse, la proposition énoncée se trouve établie.

Nous observerons qu'il serait inutile de considérer des formes (a, b, c) pour lesquelles le plus grand diviseur commun σ de leurs coefficients a, b, c différerait de l'unité, puisque de pareilles formes ne sont évidemment que des formes du déterminant $\frac{D}{\sigma^2}$, affectées du facteur entier σ . Nous supposerons donc toujours a, b, c libres de tout diviseur commun; cela étant, le plus grand diviseur commun de $a, 2b, c$, que nous désignerons constamment par ω , ne peut avoir que l'une des trois valeurs 1, $1+i$ ou 2, ce qui donne lieu à diviser les formes quadratiques en trois espèces appelées, suivant l'ordre des cas énoncés, la *première*, la *seconde* ou la *troisième*, de sorte que des formes équivalentes sont toujours de même espèce.

§. 11.

Relativement à l'équivalence des formes, il se présente deux questions principales à résoudre. Étant données deux formes ayant le même déterminant et appartenant à la même espèce, on peut demander 1^o si ces formes sont équivalentes ou non, et l'équivalence supposée reconnue, on peut se proposer 2^o d'assigner toutes les substitutions par lesquelles ces formes se transforment

l'une dans l'autre. Nous ne sommes pas pour le moment en mesure d'aborder la première de ces deux questions; mais nous pouvons traiter dès à présent la seconde, en la posant comme il suit:

„Étant données deux formes équivalentes ainsi qu'une transformation de la première dans la seconde, trouver toutes les transformations qui produisent le même effet.“

I. La question énoncée peut se réduire à une autre plus simple et qui n'est au fond qu'une question particulière, mais de même nature que la proposée. Cette question particulière consiste à assigner toutes les substitutions par lesquelles une forme donnée se change en elle-même ou, autrement dit, reste invariable quant à ses coefficients. Pour le prouver, soit:

$$(1) \quad \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

la substitution donnée par laquelle la première f des formes données se change dans la seconde f' . Si maintenant l'on désigne par:

$$(2) \quad \begin{pmatrix} \lambda, & \mu \\ \nu, & \varrho \end{pmatrix}$$

une substitution quelconque qui change en elle-même la forme f , il résulte du paragraphe précédent (II.), que par la substitution composée des précédentes, rangées dans l'ordre (2), (1):

$$(3) \quad \begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix}$$

où l'on a:

$$(4) \quad \begin{cases} \alpha' = \alpha\lambda + \gamma\mu, & \beta' = \beta\lambda + \delta\mu, \\ \gamma' = \alpha\nu + \gamma\varrho, & \delta' = \beta\nu + \delta\varrho, \end{cases}$$

f se change en f' . Cela posé, je dis que, si dans les équations (4) on introduit successivement toutes les substitutions (2), on obtiendra toutes les transformations possibles de f en f' , et de plus que chacune d'entre elles ne se présentera ainsi qu'une seule fois. Pour prouver d'abord ce dernier point, il suffit d'observer que les équations (4), en y considérant $\lambda, \mu, \nu, \varrho$ comme des inconnues, donnent ces valeurs complètement déterminées:

$$\begin{aligned} \lambda &= \delta\alpha' - \gamma\beta', & \mu &= \alpha\beta' - \beta\alpha', \\ \nu &= \delta\gamma' - \gamma\delta', & \varrho &= \alpha\delta' - \beta\gamma'. \end{aligned}$$

Reste à faire voir qu'il n'existe aucune transformation $\begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix}$ de f en f' , qui

ne soit contenue dans les formules (4), en y considérant λ, μ, ν, ρ généralement comme les coefficients des substitutions (2) définies plus haut.

Comme la résolution des équations en question a donné des valeurs entières, et que d'un autre côté, on conclut de l'équation identique:

$$(\lambda\rho - \mu\nu)(\alpha\delta - \beta\gamma) = \alpha'\delta' - \beta'\gamma',$$

combinée avec celles-ci:

$$\alpha\delta - \beta\gamma = 1, \quad \alpha'\delta' - \beta'\gamma' = 1,$$

que l'on a aussi $\lambda\rho - \mu\nu = 1$, tout revient évidemment à s'assurer que la substitution $\begin{pmatrix} \lambda & \mu \\ \nu & \rho \end{pmatrix}$ formée avec les entiers λ, μ, ν, ρ , donnés par la résolution effectuée, est en effet l'une de celles qui changent la forme f en elle-même. Désignant pour un instant par χ la forme encore inconnue dans laquelle f se transforme par la substitution dont il s'agit, on voit d'abord que χ devient f' au moyen de la substitution $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, et que par suite f' se change en χ au moyen de la substitution inverse $\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$. Mais d'un autre côté, cette dernière change aussi f' en f , d'où il suit qu'on a $f = \chi$, ce qu'il s'agissait de prouver.

II. Tout se réduit donc à découvrir toutes les substitutions $\begin{pmatrix} \lambda & \mu \\ \nu & \rho \end{pmatrix}$ par lesquelles la forme donnée $f = (a, b, c)$ se change en elle-même. Pour résoudre cette question, il s'agira d'assigner toutes les valeurs entières λ, μ, ν, ρ telles qu'en remplaçant dans l'expression:

$$ax^2 + 2bxy + cy^2,$$

ou ce qui revient au même, a différant de zéro, dans celle-ci:

$$a(ax^2 + 2bxy + cy^2),$$

x et y respectivement par $\lambda x + \mu y$ et $\nu x + \rho y$, cette expression reste identiquement la même. Nous ferons d'abord abstraction de la condition $\lambda\rho - \mu\nu = 1$, toujours exigée dans les transformations que nous employons, et de plus nous considérerons λ, μ, ν, ρ comme susceptibles de valeurs rationnelles quelconques. La question ainsi généralisée une fois résolue, il sera facile d'avoir égard aux conditions jusque-là négligées.

L'expression dont il s'agit, se décompose en ces deux facteurs linéaires:

$$(ax + (b + \sqrt{D})y), \quad (ax + (b - \sqrt{D})y),$$

où nous entendons par \sqrt{D} une valeur déterminée, mais qui peut être arbitrairement choisie parmi les deux valeurs opposées que comporte généralement un radical carré. La substitution indiquée change le produit précédent en celui-ci :

$$[(a\lambda + br + r)\sqrt{D}]x + (a\mu + bq + q\sqrt{D})y][(a\lambda + br - r)\sqrt{D}]x + (a\mu + bq - q\sqrt{D})y].$$

Désignant pour un instant les huit coefficients de x et y par des lettres particulières, en posant :

$$p = a, \quad q = b + \sqrt{D}, \quad \dots, \quad p' = a\lambda + br + r\sqrt{D}, \quad q' = a\mu + bq + q\sqrt{D}, \quad \dots$$

l'égalité qu'il s'agit d'établir entre ces deux produits, s'écrira ainsi :

$$(px + qy)(rx + sy) = (p'x + q'y)(r'x + s'y).$$

Or, les quatre constantes p, q, r, s données étant évidemment toutes différentes de zéro, les conditions nécessaires et suffisantes pour l'identité de ces deux expressions exigent évidemment qu'on ait 1^o $\frac{p'r'}{pr} = 1$, et en outre 2^o l'un ou l'autre de ces deux systèmes d'équations :

$$\frac{p'}{p} = \frac{q'}{q}, \quad \frac{r'}{r} = \frac{s'}{s}; \quad \frac{r'}{p} = \frac{s'}{q}, \quad \frac{p'}{r} = \frac{q'}{s}.$$

Si maintenant, suivant qu'il s'agit du premier ou du second cas, on pose :

$$\frac{p'}{p} = g + \psi\sqrt{D}, \quad \text{ou} \quad \frac{r'}{p} = g + \psi\sqrt{D},$$

où nous supposons g et ψ rationnels, ce qui est permis, les coefficients p, q, \dots ne renfermant que la seule irrationnelle \sqrt{D} , on aura respectivement :

$$\frac{r'}{r} = g - \psi\sqrt{D}, \quad \text{ou} \quad \frac{p'}{r} = g - \psi\sqrt{D},$$

et l'équation $\frac{p'r'}{pr} = 1$, commune aux deux cas, prendra la forme :

$$(5) \quad g^2 - D\psi^2 = 1.$$

Quant à l'autre condition, exprimée par deux équations, il suffit d'écrire pour l'un et l'autre cas, la première de ces deux équations, celle-ci comprenant virtuellement la seconde qui n'en diffère que par le signe du radical.

On aura donc suivant les deux cas :

$$\frac{a\lambda + br + r\sqrt{D}}{a} = \frac{a\mu + bq + q\sqrt{D}}{b + \sqrt{D}} = g + \psi\sqrt{D},$$

ou :

$$\frac{a\lambda + br - r\sqrt{D}}{a} = \frac{a\mu + bq - q\sqrt{D}}{b + \sqrt{D}} = g + \psi\sqrt{D}.$$

En égalant séparément dans ces formules les parties rationnelles et les coefficients de \sqrt{D} , et résolvant ensuite les équations que l'on obtient ainsi, par rapport à $\lambda, \mu, \nu, \varrho$, on trouve sans indétermination et suivant les deux cas :

$$\left. \begin{aligned} \lambda &= g - b\psi, & \mu &= -c\psi, \\ r &= a\psi, & \varrho &= g + b\psi, \end{aligned} \right| \left. \begin{aligned} \lambda &= g + b\psi, & \mu &= \frac{2b}{a}g + \frac{b^2 + D}{a}\psi, \\ r &= -a\psi, & \varrho &= -g - b\psi. \end{aligned} \right.$$

On voit donc que toutes les valeurs rationnelles $\lambda, \mu, \nu, \varrho$ qui satisfont à la condition d'invariabilité exigée, sont données par ces deux systèmes de formules très simples, où g et ψ désignent généralement toutes les valeurs rationnelles simultanées compatibles avec l'équation (5).

Il s'agit maintenant d'avoir égard aux conditions que nous avons négligées, et dont l'une est exprimée par l'équation $\lambda\varrho - \mu\nu = 1$. La substitution des expressions précédentes montre, par un calcul très simple, que le premier système y satisfait, tandis que relativement au second, on trouve $\lambda\varrho - \mu\nu = -1$. Ce dernier devant ainsi être rejeté, il ne reste plus qu'à examiner sous quelles conditions les expressions de $\lambda, \mu, \nu, \varrho$, données par le premier système, sont entières. Il est facile de voir que cela exige que les produits $\omega g, \omega\psi$ (ω désignant toujours le plus grand diviseur commun de $a, 2b, c$) soient des entiers. En effet, comme des équations précédentes on conclut facilement :

$$r = \frac{a}{\omega}\omega\psi, \quad \varrho - \lambda = \frac{2b}{\omega}\omega\psi, \quad -\mu = \frac{c}{\omega}\omega\psi,$$

on voit que, si le produit $\omega\psi$, réduit à sa plus simple expression, avait un dénominateur autre que l'unité, ce dénominateur serait diviseur commun des entiers $\frac{a}{\omega}, \frac{2b}{\omega}, \frac{c}{\omega}$, qui n'admettent pas de pareil diviseur. La conclusion obtenue pour $\omega\psi$, s'étend à ωg , au moyen de l'équation $\omega g = \omega\lambda + b\omega\psi$. Mais la réciproque a également lieu, et il est facile de s'assurer que, si l'on fait usage de valeurs de g et ψ , telles que $g = \frac{t}{\omega}, \psi = \frac{u}{\omega}$, où t et u sont des entiers, et satisfaisant à l'équation (5), il en résultera des valeurs entières pour $\lambda, \mu, \nu, \varrho$. Pour le voir, substituons ces expressions dans les équations obtenues plus haut; il viendra ainsi :

$$(6) \quad t^2 - Du^2 = \omega^2,$$

$$(7) \quad \lambda = \frac{t - bu}{\omega}, \quad \mu = -\frac{cu}{\omega}, \quad r = \frac{au}{\omega}, \quad \varrho = \frac{t + bu}{\omega}.$$

Relativement à μ et ν il n'y a rien à prouver, a et c étant divisibles par ω . Quant à λ et ϱ , comme leur différence $\varrho - \lambda = \frac{2bu}{\omega}$ est évidemment un entier, tout revient à faire voir que l'une des expressions $\frac{t+bu}{\omega}$, $\frac{t-bu}{\omega}$ est pareillement un entier. Mais de l'équation à laquelle t et u sont supposés satisfaire, mise sous la forme:

$$\frac{(t+bu)(t-bu)}{\omega^2} = 1 - \frac{ac}{\omega^2} u^2,$$

on conclut que le produit des deux facteurs $t+bu$ et $t-bu$ est un multiple de ω^2 , d'où et de ce que ω ne renferme pas plusieurs nombres premiers différents, il suit que l'un au moins des deux facteurs est divisible par ω , ce qu'il s'agissait de faire voir. Les formules (7), en y substituant successivement toutes les solutions entières de l'équation (6), donneront donc toutes les transformations $\begin{pmatrix} \lambda & \mu \\ r & \varrho \end{pmatrix}$ de la forme (a, b, c) en elle-même, et il est d'ailleurs évident que chacune de ces transformations ne se présentera qu'une seule fois, car on voit par les deux premières des formules en question qu'à des valeurs déterminées λ et μ répondent toujours des valeurs également déterminées pour t et u .

Remarque. L'analyse qui vient de nous conduire de la manière la plus simple à la solution de la question proposée, a en outre l'avantage de montrer clairement ce qui distingue les transformations propres, les seules que nous ayons à considérer, de celles qu'on appelle impropres. On voit en effet que, s'il s'agit des transformations d'une forme en elle-même, les premières sont celles pour lesquelles les deux expressions linéaires dont la forme donnée peut être considérée comme le produit, restent l'une et l'autre invariables, abstraction faite des facteurs constants qu'elles acquièrent; tandis que les transformations impropres qui n'existent toutefois que pour des formes d'une nature particulière et répondent alors au second des deux systèmes d'équations obtenus plus haut, ont pour effet d'échanger entre elles les deux expressions linéaires dont il s'agit. La même remarque s'étend aux substitutions qui ne reproduisent pas la forme donnée, et la changent au contraire en une autre équivalente, mais distincte. En combinant ce qui précède avec le résultat du numéro précédent, il est facile de s'assurer que, si après avoir décomposé en facteurs linéaires la forme primitive et celle qui en dérive, on considère comme correspondants ceux de leurs facteurs qui contiennent le radical \sqrt{D} avec le même signe, toute transformation

de la première dans la seconde sera propre ou impropre, suivant que les facteurs linéaires se changent en leurs correspondants ou non.

III. Si maintenant nous substituons les expressions (7) dans les équations (4), ces dernières prendront la forme:

$$\begin{aligned} \alpha' &= \frac{\alpha t - (b\alpha + c\gamma)u}{\omega}, & \beta' &= \frac{\beta t - (b\beta + c\delta)u}{\omega}, \\ \gamma' &= \frac{\gamma t + (a\alpha + b\gamma)u}{\omega}, & \delta' &= \frac{\delta t + (a\beta + b\delta)u}{\omega}. \end{aligned}$$

Au moyen de ces équations, on pourra donc, une première transformation $\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix}$ d'une forme (a, b, c) en une autre $(\alpha', \beta', \gamma')$ équivalente étant donnée, en déduire toutes les transformations possibles, en supposant d'ailleurs que la solution complète de l'équation (6) soit également connue.

§. 12.

Lorsque la forme:

$$(1) \quad ax^2 + 2bxy + cy^2,$$

dont nous désignerons le déterminant par D , et dont nous considérerons d'abord les coefficients a, b, c comme susceptibles d'un diviseur commun quelconque, obtient une valeur déterminée m , en y attribuant des valeurs particulières r et s aux indéterminées x et y , nous dirons que l'entier m est *représenté* par la forme donnée. Nous supposerons toujours, si nous n'avertissons expressément du contraire, que les entiers déterminés r et s sont premiers entre eux. Sous cette restriction, m diffère toujours de zéro: car il est facile de voir que l'hypothèse de $m = 0$ suppose $r = 0, s = 0$, valeurs dont un nombre quelconque est diviseur commun. Il s'agit maintenant de déduire les conséquences qui résultent d'une représentation telle que nous venons de la définir. On voit tout d'abord que, si l'on choisit deux entiers ρ et σ qui satisfassent à l'équation:

$$(2) \quad r\sigma - s\rho = 1,$$

évidemment résoluble, et que l'on applique ensuite la substitution $\begin{pmatrix} \rho, \sigma \\ s, \sigma \end{pmatrix}$ à la forme (1), elle se changera en cette autre équivalente:

$$(3) \quad \left(m, n, \frac{n^2 - D}{m} \right),$$

où:

$$(4) \quad m = ar^2 + 2brs + cs^2, \quad (5) \quad n = arq + b(r\sigma + s\rho) + cs\sigma.$$

Le troisième coefficient de la forme (3) étant entier, on conclut que n satisfait à la congruence:

$$(6) \quad z^2 \equiv D \pmod{m}.$$

On voit donc qu'une condition nécessaire, quoique nullement suffisante, pour que m puisse être représenté par la forme (1), consiste en ce que D doit être résidu quadratique relativement au module m , et que d'une représentation supposée connue, on peut toujours déduire une racine n de la congruence (6), en substituant une solution quelconque de l'équation (2) dans la formule (5). Comme l'équation (2) admet toujours une infinité de solutions, il est naturel de rechercher comment n varie, lorsqu'on passe d'une de ces solutions à une autre. Pour y parvenir, soit q_0, σ_0 une solution particulière et soit n_0 la valeur correspondante de n ; si maintenant l'on introduit dans la formule (5) la solution générale $q = q_0 + r\xi, \sigma = \sigma_0 + s\xi$, où ξ désigne un entier complexe arbitraire, on aura pour la valeur générale de n :

$$n = n_0 + m\xi,$$

d'où l'on conclut que les valeurs en nombre infini dont n est susceptible, forment une racine unique de la congruence (6), puisqu'elles sont toutes congrues entre elles suivant le module m , et l'on doit ajouter que l'arbitraire ξ peut toujours être choisie de manière à faire coïncider n avec l'une quelconque des valeurs en nombre infini, que l'on peut considérer comme autant d'expressions différentes d'une même racine de la congruence en question.

Cela étant, nous dirons désormais d'une manière abrégée, que la représentation de l'entier m par la forme (1), pour laquelle on a $x = r, y = s$, appartient à la valeur n de l'expression $\sqrt{D} \pmod{m}$, que l'on déduit de l'équation (5), en y substituant deux quelconques des entiers q et σ qui satisfont à l'équation (2).

La conclusion que nous venons d'obtenir et qui consiste en ce que la représentation $x = r, y = s$, appartenant à la valeur n de $\sqrt{D} \pmod{m}$, a toujours pour conséquence l'équivalence des formes (1) et (3), a également lieu en sens inverse. En effet si, supposant l'équivalence de ces dernières, nous

désignons par $\begin{pmatrix} r, & \varrho \\ s, & \sigma \end{pmatrix}$ l'une quelconque des substitutions par lesquelles la première se change dans la seconde, nous aurons évidemment les équations (2), (4) et (5), dont la seconde fournit une représentation qui, en vertu des deux autres, appartient évidemment à la valeur n de $\sqrt{D} \pmod{m}$. Je dis de plus qu'il n'y a aucune représentation satisfaisant à la condition exigée, qui ne puisse s'obtenir ainsi au moyen d'une transformation de la forme (1) en (3), et que chaque représentation se présentera une seule fois, c'est-à-dire qu'elle proviendra toujours d'une transformation unique et déterminée. Pour prouver d'abord le premier point, remarquons qu'en vertu de la définition même de la valeur n à laquelle une représentation est dite appartenir, supposer l'existence d'une telle représentation pour l'entier m , c'est supposer les équations (4), (2) et (5), desquelles il résulte sur-le-champ que la forme (1), au moyen de la substitution $\begin{pmatrix} r, & \varrho \\ s, & \sigma \end{pmatrix}$, se change en une autre du même déterminant D , et dont les deux premiers coefficients sont m et n . On conclut de là que le troisième coefficient est $\frac{n^2-D}{m}$, et que la substitution indiquée est en effet l'une de celles par lesquelles la forme (1) se change en (3). Quant au second point, il est évident que pour l'établir, on n'a qu'à faire voir que les deux équations (2) et (5), en y considérant r et s comme donnés, ne sauraient être satisfaites par plus d'un couple de valeurs de ϱ et de σ . Mais cela est manifeste, puisque les équations dont il s'agit, étant résolues, donnent ces valeurs complètement déterminées:

$$\varrho = \frac{(n-b)r - cs}{m}, \quad \sigma = \frac{ar + (n+b)s}{m}.$$

On voit par ce qui précède, que pour que l'entier m puisse être représenté par la forme (1) de manière que ces représentations appartiennent à une valeur donnée n de l'expression $\sqrt{D} \pmod{m}$, il faut et il suffit que les formes (1) et (3) soient équivalentes entre elles. Cette condition supposée remplie, on n'aura plus qu'à chercher toutes les substitutions $\begin{pmatrix} r, & \varrho \\ s, & \sigma \end{pmatrix}$ par lesquelles la forme (1) se change en (3), et l'on posera $x = r$, $y = s$. Or, les substitutions dont il s'agit ayant été exprimées dans le paragraphe précédent en fonction de l'une quelconque d'entre elles, on en conclut, si nous revenons maintenant à l'hypothèse que les coefficients de la forme (1) n'ont pas de di-

viséur commun, que les représentations cherchées sont toutes comprises dans ces deux équations:

$$x = \frac{\alpha t - (b\alpha + c\gamma)u}{\omega}, \quad y = \frac{\gamma t + (a\alpha + b\gamma)u}{\omega},$$

où α, γ appartiennent à une substitution $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ arbitrairement choisie parmi celles qui transforment la forme (1) en (3), et où t et u satisfont généralement à l'équation $t^2 - Du^2 = \omega^2$. Il est bon de remarquer que le résultat est maintenant tout-à-fait indépendant de la forme (3) que nous avons eu à considérer pour l'obtenir. En effet, comme $x = \alpha, y = \gamma$ est évidemment une représentation particulière comprise dans les formules précédentes et qui s'en déduit en supposant $t = \omega, u = 0$, on peut l'énoncer en disant que les équations que nous venons d'obtenir, expriment toutes les représentations appartenant à une même valeur de $\sqrt{D} \pmod{m}$, en fonction de l'une quelconque d'entre elles.

§. 13.

Les questions que nous avons traitées dans les paragraphes précédents, s'étant trouvées dépendre de la solution de l'équation indéterminée:

$$t^2 - Du^2 = \omega^2,$$

il est temps de nous occuper de cette dernière. Mais pour ne pas donner une étendue démesurée au présent Mémoire, nous considérerons exclusivement le cas où $\omega = 1$, cas qui est celui des formes de première espèce; et nous laisserons au lecteur qui voudrait s'exercer sur ces matières, le soin de chercher les modifications assez légères qu'il faudrait apporter aux recherches suivantes pour les rendre applicables aux formes des deux autres espèces.

La théorie de l'équation:

$$t^2 - Du^2 = 1$$

peut se déduire d'un lemme dont voici l'énoncé:

« a désignant un nombre complexe irrationnel donné, on pourra toujours trouver une infinité d'entiers complexes simultanés x et y , tels qu'on ait:

$$N(x - ay) < \frac{4}{N(y)}. »$$

Observons d'abord que, si l'on satisfait à la condition du lemme par le système

x , y , on y satisfera aussi par $i^s x$, $i^s y$. Comme dans l'application que nous aurons à faire du lemme, il importe de ne pas employer simultanément des systèmes dérivant ainsi l'un de l'autre, nous éviterons cet inconvénient, en ne considérant deux systèmes comme distincts qu'autant que les valeurs de $N(x-ay)$ qui s'y rapportent, sont différentes entre elles. Il est en effet évident que pour deux systèmes comme ceux dont il vient d'être question, l'expression $N(x-ay)$ a toujours la même valeur. On voit encore que la condition du lemme se trouve remplie lorsque, x étant quelconque, on a $y = 0$; mais nous ferons par-là abstraction de ce cas, de sorte que $x-ay$ aura toujours une valeur irrationnelle et par conséquent différente de zéro.

Pour démontrer notre lemme, commençons par faire voir qu'on peut toujours trouver deux entiers x et y , qui satisfaisant à l'inégalité proposée, soient en outre tels que l'on ait :

$$N(x-ay) < A.$$

A désignant une quantité positive arbitrairement choisie. Soit à cet effet n un entier positif pour lequel on ait $A > \frac{1}{2n^2}$, et désignons par η l'un quelconque des entiers complexes dont les deux parties, et j'entends par là la partie réelle et le coefficient de i qui entrent dans une expression complexe quelconque, soient comprises dans la suite :

$$-n, -(n-1), \dots, -1, 0, +1, \dots, n-1, n.$$

Relativement à chacun des entiers η dont le nombre est évidemment égal à $(2n+1)^2$, déterminons l'entier correspondant ξ tel que les deux parties de l'expression :

$$\xi - a\eta$$

obtiennent des valeurs non-négatives et inférieures à l'unité. Cela supposé, il est évident que, si l'on désigne par :

$$p \frac{1}{2n}, \quad q \frac{1}{2n}$$

les plus grands multiples de $\frac{1}{2n}$, respectivement contenus dans les deux parties dont il s'agit, les entiers réels p et q seront l'un et l'autre compris dans la suite :

$$0, 1, 2, \dots, 2n-1.$$

Or, comme avec de pareils entiers on ne peut former qu'un nombre de combinaisons distinctes, exprimé par $(2n)^2$, tandis que celui des expressions $\xi - a\eta$ est $(2n+1)^2$, on voit que l'une au moins des combinaisons p, q devra se reproduire. Soient donc:

$$\xi - a\eta, \quad \xi' - a\eta'$$

les deux expressions ou deux des expressions pour lesquelles cette circonstance se présente: il est évident qu'en formant la différence de ces expressions, on obtiendra, en posant:

$$\xi - \xi' = x, \quad \eta - \eta' = y,$$

une nouvelle expression:

$$x - ay,$$

dans laquelle l'entier y sera évidemment différent de zéro, et dont les deux parties seront, abstraction faite du signe, inférieures à $\frac{1}{2n}$, de sorte qu'on aura:

$$N(x - ay) < \frac{1}{2n^2}, \quad \text{et par suite } N(x - ay) < A,$$

ce qui coïncide avec la seconde des conditions posées plus haut. Pour prouver que l'expression $N(x - ay)$ satisfait aussi à l'autre condition qui est celle du lemme, observons que, les deux parties de $y = \eta - \eta'$ ayant évidemment des valeurs numériques non-supérieures à $2n$, on a l'inégalité $N(y) \leq 8n^2$, dont la comparaison avec celle que nous venons d'obtenir, donne:

$$N(x - ay) < \frac{4}{N(y)},$$

conformément à l'énoncé.

Ayant ainsi prouvé qu'on peut toujours trouver un couple x, y qui, en même temps qu'il s'accorde avec la condition de l'énoncé, satisfasse à l'inégalité $N(x - ay) < A$, où A est d'une petitesse arbitraire, il est facile d'en conclure la vérité du lemme. Il suffit pour cela d'observer que, quel que soit le nombre des systèmes qu'on suppose déjà connus, on trouvera un nouveau système distinct des premiers si, appliquant le procédé que nous venons d'exposer, on y suppose A égal à la plus petite des valeurs que l'expression $N(x - ay)$ présente dans les systèmes antérieurement obtenus.

Remarquons maintenant que, relativement à deux quantités complexes quelconques r et s , on a l'inégalité connue et d'ailleurs facile à vérifier:

$$|\overline{N(r+s)}| \leq |\overline{N(r)}| + |\overline{N(s)}|.$$

les radicaux étant supposés pris positivement. Supposant $r = x - ay$, $s = 2ay$, il viendra :

$$\sqrt{N(x+ay)} \leq \sqrt{N(x-ay)} + \sqrt{N(2ay)},$$

inégalité qui au moyen de celle du lemme, mise sous la forme :

$$\sqrt{N(x-ay)} < \frac{2}{\sqrt{N(y)}},$$

se change en :

$$\sqrt{N(x+ay)} < 2\sqrt{N(ay)} + \frac{2}{\sqrt{N(y)}}.$$

Ces deux dernières étant multipliées entre elles, donnent :

$$\sqrt{N(x^2 - a^2y^2)} < 4\sqrt{N(a)} + \frac{4}{\sqrt{N(y)}}$$

et par suite, y étant un entier complexe différent de zéro de sorte que $N(y) \geq 1$:

$$\sqrt{N(x^2 - a^2y^2)} < 4(\sqrt{N(a)} + 1).$$

On voit donc que pour tous les couples d'entiers qui satisfont au lemme et dont le nombre est infini, $N(x^2 - a^2y^2)$ reste au-dessous d'une limite invariable. Appliquons ce résultat au cas où $a = \sqrt{D}$, D étant un entier complexe non-carré et le radical désignant une racine déterminée qui restera toujours la même dans ce qui va suivre. Comme dans cette hypothèse, $x^2 - a^2y^2 = x^2 - Dy^2$ est un entier complexe et qu'il n'y a qu'un nombre fini d'entiers dont la norme soit inférieure à une limite donnée, il faudra nécessairement que l'expression $x^2 - Dy^2$ obtienne une infinité de fois une même valeur l qui sera évidemment différente de zéro, y n'étant pas nul. L'équation $x^2 - Dy^2 = l$ étant ainsi satisfaite par un nombre infini de systèmes x, y , on voit encore que parmi ces systèmes il s'en trouvera nécessairement un nombre illimité, pour lesquels les valeurs tant de x que de y présentent des différences multiples de l . Soient :

$$x^2 - Dy^2 = l, \quad x'^2 - Dy'^2 = l$$

deux équations pour lesquelles cela arrive, de sorte qu'on ait simultanément $x \equiv x', y \equiv y' \pmod{l}$. Le produit de ces équations étant :

$$(xx' - Dyy')^2 - D(xy' - yx')^2 = l^2,$$

et $xy' - yx'$ étant divisible par l en vertu des conditions supposées, $xx' - Dyy'$ sera aussi un multiple de l , de sorte qu'en divisant par l^2 , on aura :

$$t^2 - Du^2 = 1,$$

les entiers t et u étant donnés par les formules:

$$t = \frac{xx' - Dyy'}{l}, \quad u = \frac{xy' - yx'}{l}.$$

Nous ajouterons qu'il ne saurait arriver qu'on eût $u = 0$, car il est facile de se convaincre que cela supposerait $x' = \pm x$, $y' = \pm y$, de sorte que les systèmes x, y et x', y' ne seraient pas distincts.

Étant ainsi assuré que l'équation $t^2 - Du^2 = 1$ est toujours résoluble sans qu'on suppose $u = 0$, on parviendra nécessairement à une solution si l'on attribue successivement à u toutes les valeurs entières dont les normes forment la suite croissante des entiers positifs susceptibles d'être décomposés en deux carrés, jusqu'à ce que l'on tombe sur une valeur de u pour laquelle $Du^2 + 1$ soit égal à un carré. Cette simple possibilité suffit pour notre objet. Il existe un algorithme assez expéditif et analogue à celui des fractions continues, au moyen duquel on peut obtenir toutes les solutions de l'équation proposée ou plutôt celle de ces solutions, que l'on doit considérer comme fondamentale et dont les autres se déduisent facilement; mais comme l'exposition de cet algorithme exigerait de longs détails qui ne sont nullement nécessaires pour le but que nous avons en vue, nous ne nous en occuperons pas ici.

§. 14.

La possibilité de l'équation:

$$(1) \quad t^2 - Du^2 = 1$$

ayant été établie dans le paragraphe précédent, il s'agira maintenant de découvrir le lien qui existe entre ses solutions en nombre infini. C'est à quoi nous parviendrons par les considérations suivantes.

I. Observons d'abord que la double solution évidente $t = \pm 1$, $u = 0$ est la seule pour laquelle l'une des indéterminées soit égale à zéro. Car il est manifeste que l'hypothèse $t = 0$ est inadmissible, D n'étant pas un carré. Pour cette solution on a $N(t + u\sqrt{D}) = 1$, et je dis de plus qu'elle est la seule pour laquelle cette équation ait lieu. En effet, comme les expressions $N(t + u\sqrt{D})$, $N(t - u\sqrt{D})$ ont toujours des valeurs réciproques l'une de l'autre, puisque l'on a:

$$N(t + u\sqrt{D})N(t - u\sqrt{D}) = N(t^2 - Du^2) = 1,$$

la condition précédente est équivalente à celle-ci:

$$N(t+u\sqrt{D})+N(t-u\sqrt{D}) = 2.$$

Si maintenant l'on remarque que, r et s étant des quantités complexes quelconques, on a identiquement:

$$N(r+s)+N(r-s) = 2N(r)+2N(s),$$

cette dernière pourra prendre la forme:

$$N(t)+N(u)N(\sqrt{D}) = 1.$$

Or, $N(\sqrt{D})$ étant une quantité égale ou supérieure à l'unité, cette équation exige évidemment que l'on ait $u = 0$, ou $t = 0$ lorsque $N(D) = 1$: mais la dernière hypothèse ne pouvant avoir lieu, l'assertion avancée se trouve justifiée.

II. Je dis en second lieu que, si pour deux solutions t, u et t', u' on a $N(t'+u'\sqrt{D}) = N(t+u\sqrt{D})$, ces deux solutions sont ou identiques ou opposées, de sorte que $t' = \pm t$, $u' = \pm u$, les signes se correspondant. En effet il est clair que de deux solutions quelconques t, u et t', u' on peut en déduire une troisième au moyen de l'équation:

$$\frac{t'+u'\sqrt{D}}{t+u\sqrt{D}} = r+v\sqrt{D},$$

dans laquelle il faut égarder séparément les parties rationnelles et les coefficients de \sqrt{D} , ce qui donne:

$$r = tt' - Duu', \quad v = tu' - ut'.$$

Comme, relativement à cette nouvelle solution, on a:

$$N(r+v\sqrt{D}) = \frac{N(t'+u'\sqrt{D})}{N(t+u\sqrt{D})} = 1,$$

et par suite $r = \pm 1$, $v = 0$, on conclut $t' = \pm t$, $u' = \pm u$, ce qu'il s'agissait de prouver.

III. Si l'on excepte la double solution $t = \pm 1$, $u = 0$, les solutions de l'équation (1) existent toujours par groupes de quatre, les indéterminées pouvant être prises avec un signe arbitraire. Il est évident que relativement à un pareil groupe, l'expression $t+u\sqrt{D}$ a quatre valeurs distinctes exprimées par $\pm\chi, \pm\frac{1}{\chi}$, χ désignant l'une quelconque d'entre elles, tandis que

$N(t+u\sqrt{D})$ ne présente que ces deux valeurs distinctes: $N(\chi)$, $N\left(\frac{1}{\chi}\right)$, réciproques l'une de l'autre. L'expression $N(t+u\sqrt{D})$ n'ayant qu'une valeur unique supérieure à l'unité pour chaque groupe, cette valeur pourra servir à caractériser ce groupe et à le distinguer de tous les autres, comme cela résulte du numéro précédent où l'on a vu que la supposition $N(t+u\sqrt{D}) = N(t'+u'\sqrt{D})$ ne peut avoir lieu que pour des solutions identiques ou opposées, c'est-à-dire appartenant au même groupe. Cela posé, nous appellerons *groupe fondamental* celui pour lequel la valeur de $N(t+u\sqrt{D})$, toujours supposée supérieure à l'unité, est moindre que la valeur analogue relative à tout autre groupe. Si maintenant l'on remarque que, la variable positive ϱ étant supposée croître à partir de $\varrho = 1$, la fonction $\varrho + \frac{1}{\varrho}$ croîtra également à partir de la valeur 2, on voit que la définition précédente revient à dire que le groupe fondamental est celui pour lequel l'expression:

$$N(t+u\sqrt{D}) + \frac{1}{N(t+u\sqrt{D})} = N(t+u\sqrt{D}) + N(t-u\sqrt{D}) = 2N(t) + 2N(u)N(\sqrt{D})$$

a la plus petite valeur supérieure à 2. Sous cette forme, la définition, quoique la même au fond, a l'avantage d'être indépendante de la supposition $N(t+u\sqrt{D}) > 1$, l'expression précédente ayant évidemment la même valeur pour chacune des quatre solutions formant un même groupe. Il est actuellement facile d'indiquer une méthode propre à faire découvrir le groupe fondamental, en supposant toujours qu'il s'agisse de simples possibilités et nullement d'une opération commode sous le rapport du calcul pratique. Ayant trouvé une première solution t, u , et déterminé la valeur correspondante de $N(t+u\sqrt{D})$, désignée par b , tout revient à voir quels sont parmi les couples d'entiers t et u , tels qu'on ait:

$$1 < N(t) + N(u)N(\sqrt{D}) \leq \frac{1}{2} \left(b + \frac{1}{b} \right),$$

et qui sont évidemment en nombre fini, ceux qui, satisfaisant à l'équation (1), donnent la plus petite valeur à l'expression qui vient d'être écrite. Les quatre couples qui remplissent ces conditions, coïncident avec les quatre solutions du groupe cherché.

Il nous reste à faire voir comment de l'une des solutions de ce groupe l'on peut déduire toutes les solutions de la proposée. Quoique cela puisse se

faire au moyen de l'une quelconque d'entre elles, nous conviendrons, pour éviter des distinctions tout-à-fait inutiles, de nous servir constamment de l'une des deux solutions opposées pour lesquelles on a $N(t+u\sqrt{D}) > 1$. Nous désignerons par T, U celle des solutions fondamentales que nous emploierons et nous poserons :

$$N(T+U\sqrt{D}) = \sigma,$$

la quantité $\sigma > 1$ devant se présenter souvent dans ce qui suivra.

IV. Cela posé, je dis que toutes les solutions de l'équation (1) sont données par la formule :

$$(2) \quad t+u\sqrt{D} = \pm(T+U\sqrt{D})^n,$$

où il faut employer successivement chacun des deux signes et attribuer à l'exposant n toutes les valeurs entières depuis $-\infty$ jusqu'à ∞ , et de plus, que chaque solution est contenue d'une seule manière dans cette équation, c'est-à-dire qu'elle répond toujours à un signe et à un exposant déterminés. Il est sans doute inutile d'ajouter que pour faire usage de la formule (2), il faut évaluer séparément les parties rationnelles et les coefficients de \sqrt{D} , après avoir développé le second membre, mis préalablement sous la forme $\pm(T-U\sqrt{D})^{-n}$, lorsque n est négatif.

1°. Il est d'abord facile de prouver que les entiers t, u donnés par la formule (2), satisfont en effet à l'équation (1). Il suffit pour cela de remarquer que l'équation (2) subsiste également lorsqu'on y remplace \sqrt{D} par $-\sqrt{D}$, et que l'équation ainsi modifiée, étant multipliée par l'équation primitive, donne précisément l'équation (1).

2°. Pour faire voir en second lieu qu'il n'y a aucune solution de l'équation qui ne soit comprise dans la formule (2), posons pour un instant :

$$t_n+u_n\sqrt{D} = (T+U\sqrt{D})^n.$$

L'équation (2) est alors équivalente à ces deux équations simultanées :

$$t = \pm t_n, \quad u = \pm u_n,$$

les signes étant arbitraires, mais égaux dans les deux équations. Observons maintenant que, comme la puissance $(N(T+U\sqrt{D}))^n = \sigma^n$ croît constamment depuis la valeur zéro jusqu'à une valeur infinie, lorsque l'exposant n croît lui-même depuis $-\infty$ jusqu'à ∞ , il faut nécessairement que relativement à une

solution donnée τ, v quelconque, on ait:

$$N(\tau + v\sqrt{D}) = \sigma^n, \quad \text{ou} \quad \sigma^n < N(\tau + v\sqrt{D}) < \sigma^{n+1},$$

l'exposant n ayant une valeur unique et déterminée. Dans le premier cas, où l'on a $N(\tau + v\sqrt{D}) = N(t_n + u_n\sqrt{D})$, on conclura, en vertu du numéro II:

$$\tau = \pm t_n, \quad v = \pm u_n,$$

où le signe qui doit être le même pour les deux équations, est complètement déterminé, l'entier donné τ ne pouvant se réduire à zéro. On voit donc que pour ce premier cas, la solution donnée τ, v est comprise dans l'équation (2) et répond à un exposant et à un signe entièrement déterminés. Reste à considérer la seconde hypothèse: la double inégalité qui s'y rapporte, étant divisée par σ^n , se change en celle-ci:

$$1 < \frac{N(\tau + v\sqrt{D})}{N(t_n + u_n\sqrt{D})} < N(T + U\sqrt{D}),$$

en vertu de laquelle la nouvelle solution τ', v' donnée par la formule:

$$\tau' + v'\sqrt{D} = \frac{\tau + v\sqrt{D}}{t_n + u_n\sqrt{D}},$$

satisferait à la condition:

$$1 < N(\tau' + v'\sqrt{D}) < N(T + U\sqrt{D}),$$

ce qui est impossible, cette dernière inégalité étant en contradiction avec la définition du groupe fondamental. La seconde hypothèse ne pouvant avoir lieu, la proposition se trouve établie.

V. L'équation (1) présente deux cas particuliers qui méritent une mention spéciale comme devant donner lieu plus tard à une application très remarquable: ces cas sont ceux où D est un entier réel ou le produit d'un tel entier par i . Comme dans la théorie des nombres complexes, l'équation (1) ne diffère pas essentiellement de celle où D est remplacé par la valeur opposée, nous pouvons toujours considérer comme positif l'entier réel dont il vient d'être question.

1°. Considérons en premier lieu le cas où D est réel et positif et supposons le radical \sqrt{D} également positif. Il est évident que, si l'on satisfait alors à l'équation (1) par les valeurs $t = \alpha + \beta i, u = \gamma + \delta i$, on y satisfera aussi par celles-ci: $t = \alpha - \beta i, u = \gamma - \delta i$. Or, ces deux solutions donnant évidemment la même valeur pour l'expression $N(t + u\sqrt{D})$ sont nécessairement identiques

ou opposées, de sorte qu'on aura :

$$\alpha - \beta i = \pm(\alpha + \beta i), \quad \gamma - \delta i = \pm(\gamma + \delta i)$$

et par suite ou $\beta = 0$, $\delta = 0$ ou $\alpha = 0$, $\gamma = 0$. On voit donc que t et u sont ou l'un et l'autre des entiers réels ou l'un et l'autre de tels entiers affectés du facteur i . Il résulte de là, et en ayant égard à la formule (2), que si la solution fondamentale se trouve dans le premier cas, l'équation (1) n'a que des solutions réelles, tandis que pour une solution fondamentale imaginaire, les solutions de l'équation (1) sont en partie réelles, en partie imaginaires, les premières répondant à des valeurs paires et les dernières à des valeurs impaires de l'exposant. Si l'on observe ensuite que toute solution imaginaire de l'équation (1) donne sur-le-champ une solution réelle de $t^2 - Du^2 = -1$, et réciproquement, on peut dire que la solution fondamentale présentera le second ou le premier des deux cas indiqués, suivant que l'équation $t^2 - Du^2 = -1$ admet des solutions réelles ou non. Remarquons encore qu'en vertu de la condition $N(T + U\sqrt{D}) > 1$ à laquelle la solution fondamentale est toujours supposée satisfaire, il est évident que dans le premier cas T , U et dans le second T_1 , U_1 (en supposant $T = T_1 i$, $U = U_1 i$) sont toujours de même signe, de sorte que nous pourrions toujours considérer ces entiers comme positifs, l'inégalité précédente laissant le choix entre deux solutions fondamentales opposées. Cela posé, on voit que si dans le premier cas on n'a en vue que les solutions positives de l'équation (1), il faudra, dans la formule (2), adopter le signe supérieur et n'attribuer à n que des valeurs pareillement positives. La formule (2) ainsi restreinte donne évidemment des valeurs d'autant plus grandes pour le binôme $t + u\sqrt{D}$, et par suite pour chacun des entiers t et u , qui en vertu de l'équation (1) croissent toujours simultanément, que l'exposant n est lui-même plus grand, d'où il suit que les deux termes de la solution fondamentale T , U sont les plus petits entiers positifs qui résolvent l'équation (1).

Il serait également facile de faire voir que dans le second cas T_1 , U_1 sont les plus petits entiers positifs qui satisfont à l'équation $t^2 - Du^2 = -1$, mais il sera plus commode pour notre objet de n'employer que l'équation (1). Observons donc que pour obtenir toutes les solutions positives de cette dernière, il faudra, après avoir posé dans la formule (2) $T = T_1 i$, $U = U_1 i$, remplacer n par $2n$ et supprimer ensuite le facteur $\pm(-1)^n$. On obtient ainsi :

$$t + u\sqrt{D} = (T_1 + U_1\sqrt{D})^{2n},$$

et l'on voit alors que la plus petite solution positive de l'équation (1) est donnée par $(T_1 + U_1\sqrt{D})^2$.

En désignant donc généralement par r, v les plus petits entiers positifs qui résolvent l'équation (1), on aura suivant les deux cas:

$$r + v\sqrt{D} = T + U\sqrt{D}, \quad r + v\sqrt{D} = \left(\frac{T + U\sqrt{D}}{i}\right)^2.$$

Ces deux formules peuvent être réunies dans cette formule unique:

$$(3) \quad \sigma = N(T + U\sqrt{D}) = (r + v\sqrt{D})^z,$$

dans laquelle z désigne le nombre 1 ou le nombre 2, suivant que l'équation $t^2 - Du^2 = -1$ admet des solutions réelles ou n'en admet pas.

2^o. Pour traiter l'autre cas, soit $D = D'i$, D' étant positif. Il est facile de voir que si l'on satisfait alors à l'équation (1), en posant:

$$t = \alpha + \beta i, \quad u = \gamma + \delta i,$$

on y satisfera pareillement en posant:

$$t = \alpha - \beta i, \quad u = \delta + \gamma i.$$

Or, ces deux solutions donnant évidemment la même valeur pour l'expression $N(t) + N(u)N(\sqrt{D})$ qui, d'après ce qu'on a vu plus haut, peut servir à caractériser les différents groupes de solutions, on voit que les solutions précédentes appartiennent au même groupe. On a donc:

$$\delta + \gamma i = \pm(\gamma + \delta i)$$

et par conséquent $\delta = \pm\gamma$. Comme en vertu de ce résultat, u est toujours divisible par $1 - i$, si nous posons dans l'équation (1):

$$u = (1 - i)u', \quad t = t',$$

elle prendra la forme:

$$t'^2 - 2D'u'^2 = 1,$$

et nous retompons sur le cas déjà traité. Il est facile de conclure de là que l'expression $\sigma = N(T + U\sqrt{D})$, toujours supposée supérieure à l'unité, est pour le cas dont nous nous occupons, donnée par l'équation:

$$(4) \quad \sigma = N(T + U\sqrt{D}) = (r + v\sqrt{2D})^z,$$

r et v désignant les plus petits entiers positifs qui résolvent l'équation:

$$t'^2 - 2D'u'^2 = 1,$$

et z ayant la valeur 1 ou la valeur 2, suivant que l'équation $t'^2 - 2D'u'^2 = -1$ admet des solutions réelles ou non.

§. 15.

La théorie de l'équation $t^2 - Du^2 = 1$ étant maintenant connue, nous pouvons reprendre les questions déjà traitées plus haut et en achever la solution en nous bornant, comme nous en avons déjà averti, à considérer des formes quadratiques qui appartiennent à la première espèce.

I. Nous nous occuperons en premier lieu de celle de ces questions qui concerne les représentations d'un entier donné m par une forme (a, b, c) également donnée. Supposons que m soit susceptible d'être représenté par la forme dont il s'agit, et soient $x = \alpha$, $y = \gamma$ des valeurs particulières et premières entre elles, telles que la valeur correspondante de la forme soit égale à m . Cela posé, il résulte du §. 12 que toutes les représentations appartenant à la même valeur de l'expression $\sqrt{D} \pmod{m}$, à laquelle appartient la représentation particulière dont il s'agit, sont données par les deux équations:

$$x = \alpha t - (b + c\gamma)u, \quad y = \gamma t + (a\alpha + b\gamma)u,$$

où il faut substituer toutes les solutions de l'équation $t^2 - Du^2 = 1$. Les équations précédentes, étant respectivement multipliées par α et $b + \sqrt{D}$, et ensuite ajoutées, donnent le résultat très simple:

$$\alpha x + (b + \sqrt{D})y = (a\alpha + (b + \sqrt{D})\gamma)(t + u\sqrt{D}).$$

qui, au moyen de l'équation (2) du §. 14, se change en:

$$\alpha x + (b + \sqrt{D})y = \pm (a\alpha + (b + \sqrt{D})\gamma)(T + U\sqrt{D})^n.$$

Soit pour abrégier $N(a\alpha + (b + \sqrt{D})\gamma) = A$, et comme dans le paragraphe cité. $N(T + U\sqrt{D}) = \sigma > 1$. Cela posé, si l'on prend les normes des deux membres de l'équation précédente, on en conclura:

$$N(\alpha x + (b + \sqrt{D})y) = A\sigma^n,$$

où il importe de remarquer que chaque valeur de $N(\alpha x + (b + \sqrt{D})y)$, donnée par cette dernière équation, se présentera deux fois dans la totalité des représentations que nous considérons et que pour abrégier, nous nommerons désormais un *groupe* de représentations, comme cela résulte évidemment du double signe contenu dans l'équation précédente, et que le passage des nombres à leurs normes a fait disparaître. Observons encore que si k désigne une constante positive arbitrairement choisie, l'entier réel n qui doit croître depuis $-\infty$

jusqu'à ∞ , obtiendra évidemment une valeur et n'en obtiendra qu'une seule qui satisfasse à la double condition:

$$k < A\sigma^n \leq k\sigma.$$

On conclut de là que dans tout groupe de représentations, ou en d'autres termes, que parmi toutes les représentations qui appartiennent à une même valeur de l'expression $\sqrt{D} \pmod{m}$, il en existe toujours deux et qu'il n'en existe que deux pour lesquelles on ait:

$$k < N(ax + (b + \sqrt{D})y) \leq k\sigma,$$

et il est d'ailleurs manifeste que les deux représentations particulières dont il s'agit et qui varient avec la constante k , sont toujours telles que, l'une étant exprimée par les formules: $x = r$, $y = s$, l'autre le sera par celles-ci: $x = -r$, $y = -s$.

Le résultat que nous venons d'obtenir, va nous fournir un moyen très simple de décider 1^o si un entier donné m peut être représenté par une forme également donnée (a, b, c) ou non, et 2^o d'assigner dans le premier de ces deux cas, toutes les représentations dont m est susceptible au moyen de la forme dont il s'agit. On voit d'abord que la question proposée revient à examiner si l'on peut satisfaire à ces deux conditions simultanées:

$$(1) \quad ax^2 + 2bxy + cy^2 = m,$$

$$(2) \quad k < N(ax + (b + \sqrt{D})y) \leq k\sigma,$$

par des entiers x et y premiers entre eux. Si cela n'est pas possible, on sera assuré que m n'est pas susceptible d'être représenté par la forme donnée. Dans le cas contraire on trouvera une ou plusieurs doubles représentations telles que $x = \pm r$, $y = \pm s$; $x = \pm r'$, $y = \pm s'$; ... qui appartiendront à autant de groupes distincts, et l'on obtiendra toutes les représentations cherchées, si dans les deux équations rappelées au commencement de ce paragraphe, on pose successivement $\alpha = r$, $\gamma = s$; $\alpha = r'$, $\gamma = s'$; ...

Réduite à ce point, la question ne présente plus aucune difficulté, car il est facile de se convaincre que, pour que les entiers x et y puissent satisfaire aux conditions simultanées (1) et (2), leurs normes doivent être comprises entre certaines limites faciles à assigner, de sorte que l'examen qu'il s'agit de faire, ne doit porter que sur un nombre limité de combinaisons x, y . En effet, si après avoir multiplié par a l'équation (1), on prend les normes de ses deux

membres, il viendra :

$$N(ax+(b+\sqrt{D})y)N(ax+(b-\sqrt{D})y) = N(am).$$

Cette équation étant comparée avec la double inégalité (2), on en conclura celle-ci :

$$\frac{N(am)}{k\sigma} \leq N(ax+(b-\sqrt{D})y) < \frac{N(am)}{k},$$

et par suite en ajoutant cette dernière et l'inégalité (2) :

$$k + \frac{N(am)}{k\sigma} < 2N(ax+by) + 2N(\sqrt{D})N(y) < k\sigma + \frac{N(am)}{k}.$$

Il est facile de voir que les entiers x et y , et à plus forte raison les entiers x et y , premiers entre eux qui satisfont à cette double inégalité qui est une conséquence nécessaire des deux conditions (1) et (2), ne présentent qu'un nombre limité de combinaisons faciles à former; on pourra donc toujours décider si parmi ces entiers simultanés il en existe qui remplissent les deux conditions dont il s'agit, ce que nous nous étions proposé de faire voir.

La condition (2) qui, étant jointe à l'équation (1), a pour effet de réduire chaque groupe de représentations de l'entier m par la forme (a, b, c) à deux représentations particulières qu'elle sépare ainsi de toutes les autres, prend une forme remarquable lorsqu'on fait un choix convenable de la constante arbitraire k qu'elle contient.

Soit $k = N(\sqrt{am})$. La condition dont nous parlons, deviendra ainsi :

$$N(\sqrt{am}) < N(ax+(b+\sqrt{D})y) \leq \sigma N(\sqrt{am}).$$

Observons que, comme il ne s'agit que de quantités positives, cette double inégalité est tout-à-fait équivalente à celle-ci :

$$N(am) < (N(ax+(b+\sqrt{D})y))^2 \leq \sigma^2 N(am)$$

qui, à son tour, peut être remplacée par celle qu'on en déduit en divisant par $N(ax+(b+\sqrt{D})y)$, et en observant qu'on a :

$$N(am) = N(ax+(b+\sqrt{D})y)N(ax+(b-\sqrt{D})y).$$

On trouve ainsi :

$$(3) \quad N(ax+(b-\sqrt{D})y) < N(ax+(b+\sqrt{D})y) \leq \sigma^2 N(ax+(b-\sqrt{D})y).$$

C'est sous cette dernière forme que nous emploierons dorénavant la condition qui sert à réduire tout groupe de représentations à deux de ses termes.

II. Quant aux deux questions que nous nous étions proposées sur l'équivalence des formes, comme celle d'entre elles qui a pour objet de déduire toutes les transformations d'une forme en une autre équivalente, d'une première transformation supposée donnée, s'est trouvée dépendre de l'équation $t^2 - Dt^2 = 1$, dont nous avons donné la solution générale, nous n'avons plus à traiter que la première des questions énoncées au commencement du §. 11. Il s'agit donc de faire voir comment, étant données deux formes (a, b, c) et (a', b', c') ayant un déterminant commun D , on peut décider si ces formes sont équivalentes ou non, et obtenir, dans le premier de ces deux cas, l'une des substitutions au moyen desquelles la première se change dans la seconde. Pour résoudre cette question, on se rappellera que, d'après ce qu'on a démontré dans le §. 12, tout revient à voir s'il existe des représentations de l'entier a' par la forme (a, b, c) , qui appartiennent à la valeur b' de l'expression $\sqrt{D} \pmod{a'}$. Si l'on trouve qu'il n'y a aucune représentation pour laquelle la condition énoncée soit satisfaite, on sera assuré que les deux formes ne sont pas équivalentes; dans le cas contraire, l'une quelconque des représentations obtenues donnera sur-le-champ la transformation cherchée. La question proposée se trouvant ainsi réduite à celle dont nous avons donné la solution dans le numéro précédent de ce paragraphe, doit elle-même être considérée comme résolue.

III. Avant d'en venir à la question qui forme le principal sujet de ce Mémoire, nous avons encore à indiquer comment, étant donnée une forme $ax^2 + 2bxy + cy^2$ du déterminant D , on peut assigner d'une manière générale les valeurs simultanées x et y , pour lesquelles la valeur de cette forme soit impaire et première à D , ou plus simplement, soit première à $(1+i)D = \mathcal{A}$. Comme, en posant $x \equiv \alpha$, $y \equiv \gamma \pmod{\mathcal{A}}$, où α et γ peuvent être choisis dans un système de résidus relatif au module \mathcal{A} , on a :

$$ax^2 + 2bxy + cy^2 \equiv a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \pmod{\mathcal{A}},$$

on voit que la question proposée se réduit à examiner pour lesquelles des combinaisons α, γ ou plutôt pour combien de ces combinaisons, car c'est uniquement leur nombre qu'il nous importe de connaître, le second membre est premier à \mathcal{A} . J'observe maintenant que sans nuire en rien à la généralité de la question, il est permis de considérer le coefficient a comme premier à \mathcal{A} . En effet, comme la forme donnée est supposée de première espèce, on peut toujours, si elle ne satisfait pas à la condition énoncée, la transformer en une

autre où cette dernière se trouve remplie; et l'on prouve facilement que relativement à la nouvelle forme, le nombre des combinaisons dont il s'agit, est le même que pour la forme donnée. Le raisonnement par lequel cette dernière assertion peut être justifiée, étant très simple et d'ailleurs entièrement semblable à celui dont nous avons déjà fait usage dans la question analogue, relative aux entiers réels*), nous nous dispenserons de le répéter ici.

Cela posé, il est évident que, pour que l'expression $aa^2 + 2ba\gamma + c\gamma^2$ soit première à $\mathcal{A} = (1+i)D$, il faut et il suffit qu'il en soit de même du produit:

$$a(aa^2 + 2ba\gamma + c\gamma^2) = (aa + b\gamma)^2 - D\gamma^2.$$

Distinguons maintenant le cas où D est impair et celui où D est divisible par $1+i$. Dans le premier de ces deux cas, il faudra, si γ est divisible par $1+i$, que $aa + b\gamma$ soit premier à \mathcal{A} , et si γ est impair, que $aa + b\gamma$ soit divisible par $1+i$ et premier à D . Or comme, γ ayant une valeur déterminée, l'expression $aa + b\gamma$, dans laquelle a est le terme général d'un système de résidus pour le module \mathcal{A} , représente elle-même un semblable système (§. 5, III.), il s'agira de déterminer combien, dans un système de résidus pour le module \mathcal{A} , il existe de termes premiers à \mathcal{A} ou de termes premiers à D et en outre divisibles par $1+i$, selon que γ sera ou ne sera pas divisible par $1+i$. Le premier de ces deux nombres est $\psi(\mathcal{A})$; pour obtenir le second, on se rappellera que, si l'on divise par $1+i$ ceux des termes du système en question qui renferment le facteur $1+i$, les quotients formeront un système de résidus pour le module D (§. 5, II.), d'où l'on conclut que le nombre que nous avons à déterminer, est exprimé par $\psi(D)$. J'ajoute que cette dernière expression peut être remplacée par $\psi(\mathcal{A})$ puisque, D et $1+i$ étant premiers entre eux, on a (§. 5, V.):

$$\psi(\mathcal{A}) = \psi((1+i)D) = \psi(1+i)\psi(D) = \psi(D).$$

Ayant ainsi reconnu qu'à toute valeur déterminée γ il répond $\psi(\mathcal{A})$ valeurs a qui satisfont aux conditions exigées, et sachant d'un autre côté que γ est susceptible d'un nombre de valeurs exprimé par $N(\mathcal{A})$, on en conclura que les combinaisons a, γ qui rendent $aa^2 + 2ba\gamma + c\gamma^2$ premier à \mathcal{A} , sont au nombre de $N(\mathcal{A})\psi(\mathcal{A})$.

Le cas où D est supposé divisible par $1+i$, donne le même résultat. En effet, comme le terme $D\gamma^2$ est dans ce cas divisible par $1+i$, tout se ré-

*) Recherches sur diverses applications de l'Analyse infinitésimale à la théorie des Nombres, §. 5^o).

¹⁾ S. 437 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

duit à faire en sorte que $a\alpha + b\gamma$ soit premier à \mathcal{A} , et l'on voit facilement que les valeurs α qui, répondant à une valeur déterminée γ , satisfont à cette condition, sont toujours au nombre de $\psi(\mathcal{A})$, d'où l'on conclut que celui des combinaisons dont il s'agit, est égal à $N(\mathcal{A})\psi(\mathcal{A})$, comme dans le premier cas.

On voit ainsi que les valeurs simultanées de x et de y qui, étant substituées dans l'expression $ax^2 + 2bxy + cy^2$, la rendent première à $(1+i)D = \mathcal{A}$, peuvent toujours être distribuées en systèmes de la forme:

$$x = \mathcal{A}v + \alpha, \quad y = \mathcal{A}w + \gamma,$$

où v et w sont des entiers indéterminés, et α et γ des entiers déterminés, et que le nombre de ces systèmes est toujours exprimé par $N(\mathcal{A})\psi(\mathcal{A})$.

Classification des formes et théorèmes qui s'y rapportent.

§. 16.

La classification dont il s'agit, consiste à rapporter deux quelconques des formes qui ont un déterminant commun D , à la même classe ou à des classes distinctes, suivant que ces formes sont équivalentes ou non. Nous démontrerons d'abord que les classes ainsi définies sont toujours en nombre limité, quel que soit le déterminant donné. C'est à quoi nous parviendrons en faisant voir que dans chaque classe il existe au moins une forme (a, b, c) telle qu'on ait à la fois $\frac{1}{2}N(a) \geq N(b)$, $N(a) \leq N(c)$, et en prouvant ensuite que les formes de cette nature, qu'on appelle des formes *réduites*, sont toujours en nombre fini.

Pour établir le premier de ces deux points, il s'agira de montrer qu'une forme quelconque (a, b, a') peut toujours se transformer en une forme réduite équivalente. Considérons à cet effet la substitution $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, où nous n'avons que cette seule condition $\alpha\delta - \beta\gamma = 1$, et observons que cette dernière sera satisfaite si, δ restant quelconque, nous supposons $\alpha = 0$, $\beta = 1$, $\gamma = -1$. Au moyen de la substitution ainsi particularisée, la forme (a, b, a') se changera en une autre (a', b', a'') , où l'on aura $b' = -b - a'\delta$. D'après ce que nous avons remarqué au commencement du §. 2, nous pouvons toujours disposer de l'indéterminée δ de manière que l'on ait $\frac{1}{2}N(a') \geq N(b')$. La nouvelle forme (a', b', a'') satisfaisant alors à la première des deux conditions qui définissent les formes réduites, si l'on a en outre $N(a') \leq N(a'')$, cette forme aura toutes les propriétés requises: si non, on en déduira par le même procédé une troisième

forme (a'', b'', a''') , où l'on aura $\frac{1}{2}N(a'') \geq N(b'')$, et qui par conséquent sera une forme réduite si l'on a en outre $N(a'') \leq N(a''')$. Il est manifeste que si l'on continue à opérer toujours de la même manière, on finira nécessairement par tomber sur une forme réduite équivalente à la proposée; car pour qu'il en fût autrement, il faudrait que la suite $N(a'') > N(a''') > \dots$ pût être indéfiniment prolongée, ce qui évidemment est impossible, les entiers a', a'', a''', \dots étant tous différents de zéro si, comme on le suppose toujours, D n'est pas un carré.

Le premier point se trouvant ainsi établi, il nous reste à faire voir que les formes réduites (a, b, c) qui ont un déterminant donné D , sont en nombre limité et peuvent toujours être assignées facilement. Les deux conditions $\frac{1}{2}N(a) \geq N(b)$, $N(a) \leq N(c)$ donnent d'abord $N(ac) \geq 4N(b^2)$, et par suite $\sqrt{N(ac)} \geq 2N(b)$. Si d'un autre côté, on applique à l'équation $ac = b^2 - D$ le théorème déjà employé dans le §. 13, on en conclura :

$$\sqrt{N(ac)} \leq \sqrt{N(b^2)} + \sqrt{N(-D)},$$

ou ce qui revient au même :

$$\sqrt{N(ac)} \leq N(b) + \sqrt{N(D)},$$

inégalité qu'il suffit de comparer à celle déjà obtenue, pour voir qu'on a :

$$N(b) \leq \sqrt{N(D)}.$$

Comme $N(b)$ et par conséquent aussi b n'est ainsi susceptible que d'un nombre limité de valeurs faciles à assigner, pour obtenir toutes les formes réduites du déterminant D , il suffira de décomposer chacune des valeurs correspondantes de $b^2 - D$ de toutes les manières possibles en deux facteurs a et c , en supposant $N(a) \leq N(c)$, et de ne conserver que celles des combinaisons a, b, c pour lesquelles on a $\frac{1}{2}N(a) \geq N(b)$ *).

Ayant ainsi obtenu toutes les formes réduites (a, b, c) qui répondent à un déterminant donné, si comme nous le supposons, on n'a en vue que les formes qui appartiennent à la première espèce, il ne restera plus qu'à effacer celles des formes trouvées, pour lesquelles a, b, c ou $a, 2b, c$ auraient un diviseur commun.

*) On voit que la méthode dont nous venons de faire usage pour obtenir les formes réduites, est entièrement analogue à celle qui sert pour le même objet dans la théorie des entiers réels. Nous ajoutons que la possibilité d'appliquer cette dernière aux entiers complexes, avait déjà été remarquée par M. JACOBI (Tome XIX, p. 314 du Journal de CRELLE.)

*) Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften, Jahrgang 1839, S. 86 K.

Il s'agit maintenant de faire l'énumération complète des classes qui dépendent au déterminant D , en choisissant dans chacune de ces classes l'une quelconque des formes dont elle se compose. Des formes choisies d'après cette règle constitueront ce que nous appellerons un système complet de formes non-équivalentes ou plus simplement, *un système de formes* pour le déterminant dont il s'agit. Un tel système jouira évidemment de la double propriété de présenter une forme et de n'en présenter qu'une seule qui soit équivalente à une forme quelconque, pourvu que cette dernière ait l'entier D pour déterminant et soit d'ailleurs de première espèce. Pour construire un système de cette nature, on peut se servir des formes réduites que nous avons appris à déterminer dans ce qui précède. En effet, comme parmi les formes réduites il s'en trouve toujours au moins une, qui appartienne à une classe arbitrairement choisie, tout reviendra à éliminer les formes surabondantes. Après avoir rangé à cet effet les formes réduites dans un ordre quelconque, on commencera par comparer la première d'entre elles à chacune des suivantes et l'on effacera toutes celles de ces dernières, que l'on reconnaîtra lui être équivalentes. Cela fait, on comparera la seconde des formes que cette première opération aura laissées subsister, à chacune des suivantes pour effacer encore les formes qu'on trouvera lui être équivalentes, et ainsi de suite.

Le procédé que nous venons d'indiquer, suffit pour assigner le nombre des classes, ou ce qui revient au même, celui des termes composant un système de formes pour un déterminant quelconque, lorsque ce dernier est numériquement donné. Mais tel n'est pas l'objet principal que nous nous sommes proposé dans ce Mémoire, et qui consiste plutôt à découvrir la loi générale par laquelle le nombre des classes se trouve lié au déterminant auquel ces classes se rapportent. Pour résoudre cette dernière question, il faut pénétrer plus avant dans la nature de ce que nous avons nommé un système de formes, et se rendre compte des rapports qui existent entre un tel assemblage et la totalité des entiers que ces formes peuvent servir à représenter.

§. 17.

Soit:

$$(1) \quad ax^2 + 2bxy + cy^2, \quad a'x^2 + 2b'xy + c'y^2, \quad \dots$$

un système de formes (de première espèce) pour le déterminant D , et propo-

sous-nous de rechercher sous quelles conditions un entier m que nous supposons impair et premier à D , ou réunissant ces deux conditions en une seule, que nous supposons premier à $\mathcal{A} = (1+i)D$, peut être représenté par une ou par plusieurs de ces formes, et de déterminer, lorsque de telles représentations existent, le nombre des groupes dans lesquels leur totalité se distribue. Il est bien entendu que, comme dans ce qui précède, il n'est toujours question que de représentations pour lesquelles les indéterminées x et y soient premières entre elles. D'après le §. 12, il y a une première condition à remplir, consistant en ce que D doit être résidu quadratique à l'égard de m , et il résulte d'un autre côté du §. 9 que, pour qu'elle soit satisfaite, il faut et il suffit que pour chacun des diviseurs simples f de m , on ait:

$$(2) \quad \left[\frac{D}{f} \right] = 1.$$

Ces conditions particulières étant supposées remplies, si l'on désigne par μ le nombre des facteurs simples primaires inégaux que l'entier m contient, la congruence $z^2 \equiv D \pmod{m}$ aura 2^μ racines, et il s'agira de chercher quels sont les groupes de représentations qui puissent répondre à ces diverses racines. Soit l l'une quelconque de ces racines, et proposons-nous de déterminer les représentations qui lui appartiennent. D'après ce qui a été démontré dans le §. 12, nous avons à examiner si parmi les formes (1) il y en a une qui soit équivalente à celle-ci:

$$\left(m, l, \frac{l^2 - D}{m} \right).$$

Observons d'abord que les coefficients de cette dernière sont évidemment sans diviseur commun, puisqu'un tel diviseur diviserait aussi le déterminant D , ce qui serait contraire à l'hypothèse admise d'après laquelle m est premier à D . Comme d'un autre côté, m est supposé impair, on voit que la forme précédente appartient à la première espèce, d'où il suit que la forme dont il s'agit, a son équivalente dans le système (1). Il résulte de là et du paragraphe déjà cité, qu'il existe toujours un groupe de représentations appartenant à une racine déterminée l , et qu'il n'en existe qu'un seul, d'où l'on conclut que les représentations dont l'entier m est susceptible au moyen des expressions (1), forment toujours un nombre de groupes distincts, égal à la puissance 2^μ .

Nous pouvons maintenant réduire chacun des groupes dont il s'agit, à deux représentations individuelles, si dans chacune des formes (1), nous limitons

les indéterminées x et y , au moyen de la condition d'inégalité déjà donnée dans le §. 15, cette condition étant pour la première des expressions (1):

$$(3) \quad N(ax+(b-\sqrt{D})y) < N(ax+(b+\sqrt{D})y) \leq \sigma^2 N(ax+(b-\sqrt{D})y),$$

et se déduisant pour les autres de celle que nous venons d'écrire, en y accentuant les lettres a , b , c . Ces conditions étant jointes aux formes (1), on voit que le nombre des représentations dont m est susceptible au moyen des formes dont il s'agit, sera fini et exprimé par 2^{u+1} .

Au moyen du résultat que nous venons d'obtenir, il est facile de former l'équation générale que nous allons écrire:

$$(4) \quad \Sigma 2^{u+1} F(m) = \Sigma F(ax^2+2bxy+cy^2) + \Sigma F(a'x^2+2b'xy+c'y^2) + \dots$$

La sommation indiquée dans le premier membre est supposée embrasser la totalité des entiers m premiers à \mathcal{A} dont tous les diviseurs simples f satisfont à la condition (2), μ désignant, pour chacun de ces entiers m , le nombre de ses facteurs simples primaires inégaux. Quant aux sommes contenues dans le second membre, elles sont en même nombre que les formes (1), et répondent chacune à l'une des formes en question. Dans chacune de ces sommes le signe Σ doit s'étendre à tous les systèmes de valeurs simultanées x et y qui remplissent la triple condition de n'avoir pas de diviseur commun, de donner à la forme où elles sont substituées, une valeur première à \mathcal{A} , et enfin de satisfaire à la double inégalité (3) lorsqu'il s'agit de la première somme, et à des inégalités de même forme pour chacune des autres. La fonction désignée par la caractéristique F est arbitraire et doit seulement être choisie de manière que les séries contenues dans l'équation, soient convergentes et aient des sommes indépendantes de l'ordre de succession de leurs termes. La vérité de l'équation ainsi formée est évidente, et l'on voit que cette équation n'est que la traduction de la double propriété remarquée plus haut et consistant en ce que d'une part tout entier supposé premier à \mathcal{A} , pour être susceptible d'être représenté par les formes (1), doit être compris parmi ceux que nous venons de désigner par m , et en ce que d'autre part chacun de ces derniers admet en effet 2^{u+1} représentations au moyen des expressions (1), si à chacune de ces expressions l'on suppose jointe une condition d'inégalité comme celle de (3). D'après la manière dont l'équation précédente subsiste, il est manifeste qu'elle ne cessera pas d'avoir lieu si l'on y remplace partout les entiers complexes qui se trouvent

sous le signe F , par leurs normes, de sorte qu'on aura aussi:

$$\Sigma 2^{u+1} F(N(m)) = \Sigma F(N(ax^2+2bxy+cy^2)) + \Sigma F(N(a'x^2+2b'xy+c'y^2)) + \dots,$$

les signes sommatoires ayant toujours la même signification.

Particularisons la fonction arbitraire contenue dans l'équation, et supposons que cette fonction soit une puissance de l'exposant $-s$, où s est une quantité positive supérieure à l'unité. Il viendra ainsi:

$$\Sigma \frac{2^{u+1}}{(N(m))^s} = \Sigma \frac{1}{(N(ax^2+2bxy+cy^2))^s} + \Sigma \frac{1}{(N(a'x^2+2b'xy+c'y^2))^s} + \dots$$

Comme d'après la définition des entiers m , quatre nombres associés se trouvent évidemment toujours simultanément compris ou non parmi ces entiers m , on voit que nous pouvons considérer la sommation indiquée dans le premier membre, comme ne devant plus s'étendre qu'aux entiers m qui satisfaisant aux conditions énoncées plus haut, soient en outre primaires, c'est-à-dire tels qu'en posant $m = a + \beta i$, on ait $a \equiv 1 \pmod{4}$, $\beta \equiv 0 \pmod{2}$, pourvu qu'en même temps nous quadruplions le premier membre. On aura ainsi:

$$(5) \quad 8 \Sigma \frac{2^u}{(N(m))^s} = \Sigma \frac{1}{(N(ax^2+2bxy+cy^2))^s} + \Sigma \frac{1}{(N(a'x^2+2b'xy+c'y^2))^s} + \dots$$

L'entier m étant primaire, on aura toujours, d'une manière unique (§§. 2 et 3, V), $m = f^{h'} f^{h''} \dots$, les exposants h' , h'' , ... étant tous différents de zéro, et f' , f'' , ... désignant des nombres premiers primaires inégaux qui satisfont à la condition (2), et dont le nombre est exprimé par μ . Cela étant, il est facile de se convaincre qu'on a:

$$(6) \quad \Sigma \frac{2^u}{(N(m))^s} = H \frac{1 + \frac{1}{(N(f'))^s}}{1 - \frac{1}{(N(f'))^s}},$$

le signe H s'étendant à tous les nombres premiers impairs et primaires f , qui ne divisent pas le déterminant D et remplissent la condition (2). Il suffit de développer le facteur général comme il suit:

$$\frac{1 + \frac{1}{(N(f'))^s}}{1 - \frac{1}{(N(f'))^s}} = 1 + \frac{2}{(N(f'))^s} + \frac{2}{(N(f'')^s)} + \frac{2}{(N(f''')^s)} + \dots$$

et d'effectuer ensuite la multiplication pour reconnaître, au moyen de la remarque que nous venons de faire, que l'équation (6) est en effet exacte.

Afin de transformer ultérieurement le second membre de cette équation, soit q le terme général de la suite des nombres premiers impairs et primaires, à l'exclusion de ceux qui divisent D , et considérons le produit:

$$\Pi \frac{1}{1 - \frac{1}{(N(q))^s}}$$

où le signe de multiplication est supposé s'étendre à toutes les valeurs q que nous venons de définir. Comme l'on a:

$$\frac{1}{1 - \frac{1}{(N(q))^s}} = 1 + \frac{1}{(N(q))^s} + \frac{1}{(N(q^2))^s} + \frac{1}{(N(q^3))^s} + \dots$$

et qu'on sait d'un autre côté, que tout entier impair et primaire n'est susceptible que d'une seule décomposition en facteurs simples primaires, on voit que le produit précédent équivaut à une série d'une loi très simple, et que l'on a:

$$(7) \quad \Pi \frac{1}{1 - \frac{1}{(N(n))^s}} = \Sigma \frac{1}{(N(n))^s},$$

le signe Σ se rapportant à tous les entiers impairs n , primaires et premiers à D . Si au lieu du produit précédent, l'on considère le suivant:

$$\Pi \frac{1}{1 - \left[\frac{D}{q} \right] \frac{1}{(N(q))^s}}$$

on reconnaîtra que ce nouveau produit, traité de la même manière, se transforme en une série ayant pour terme général $\chi \frac{1}{(N(n))^s}$, où le coefficient χ sera donné par la formule:

$$\chi = \left[\frac{D}{q'} \right]^h \left[\frac{D}{q''} \right]^{h''} \dots,$$

si l'on suppose $n = q^{h'} q^{h''} \dots$, les exposants étant positifs, et q' , q'' , ... désignant les nombres premiers inégaux q que l'entier n contient. Si maintenant l'on observe qu'en vertu de la troisième des équations (e) du §. 8, l'expression χ peut être remplacée par:

$$\left[\frac{D}{q^{h'}} \right] \left[\frac{D}{q^{h''}} \right] \dots = \left[\frac{D}{q^{h'} q^{h''} \dots} \right] = \left[\frac{D}{n} \right],$$

on aura l'équation:

$$(8) \quad \Pi \frac{1}{1 - \left[\frac{D}{q} \right] \frac{1}{(N(q))^s}} = \Sigma \left[\frac{D}{n} \right] \frac{1}{(N(n))^s},$$

dans laquelle les signes \mathbf{H} et $\mathbf{\Sigma}$ ont la même signification que dans l'équation (7). Cela posé, faisons le produit des équations (7) et (8), et divisons ensuite ce produit par l'équation (7), après avoir remplacé dans cette dernière s par $2s$. Le facteur général du premier membre de l'équation que l'on obtient ainsi, sera évidemment:

$$\frac{1 - \frac{1}{(N(q))^{2s}}}{\left(1 - \frac{1}{(N(q))^s}\right) \left(1 - \left[\frac{D}{q}\right] \frac{1}{(N(q))^s}\right)} = \frac{1 + \frac{1}{(N(q))^s}}{1 - \left[\frac{D}{q}\right] \frac{1}{(N(q))^s}}.$$

Ce facteur présente deux cas différents selon que l'on a:

$$\left[\frac{D}{q}\right] = 1, \text{ ou } \left[\frac{D}{q}\right] = -1.$$

Dans le second il se réduit à l'unité et peut être omis, tandis que pour le premier il prend la forme:

$$\frac{1 + \frac{1}{(N(q))^s}}{1 - \frac{1}{(N(q))^s}}.$$

Or, les nombres premiers q pour lesquels on a $\left[\frac{D}{q}\right] = 1$, coïncidant avec ceux que nous avons précédemment désignés par f , on voit que l'équation qu'il s'agit de former, est:

$$\mathbf{H} \frac{1 + \frac{1}{(N(f))^s}}{1 - \frac{1}{(N(f))^s}} = \frac{\mathbf{\Sigma} \frac{1}{(N(n))^s} \cdot \mathbf{\Sigma} \left[\frac{D}{n}\right] \frac{1}{(N(n))^s}}{\mathbf{\Sigma} \frac{1}{(N(n))^{2s}}}.$$

Au moyen de ce résultat et de l'équation (6), l'équation (5) peut prendre la forme:

$$8 \mathbf{\Sigma} \frac{1}{(N(n))^s} \cdot \mathbf{\Sigma} \left[\frac{D}{n}\right] \frac{1}{(N(n))^s} = \mathbf{\Sigma} \frac{1}{(N(n^2))^s} \cdot \mathbf{\Sigma} \frac{1}{(N(ax^2 + 2bxy + cy^2))^s} + \dots,$$

où les signes sommatoires qui se rapportent à n , s'étendent à tous les entiers primaires et premiers à \mathcal{A} , tandis que ceux qui sont relatifs aux valeurs simultanées x et y , conservent la signification indiquée plus haut. Il est facile de se convaincre que les produits de séries, contenus dans le second membre, sont susceptibles d'une forme beaucoup plus simple, qu'ils prennent lorsque la multi-

plication indiquée est effectuée. Pour leur donner cette nouvelle forme, nous considérerons particulièrement le premier de ces produits, la même transformation s'appliquant à tous les autres. En faisant le produit des termes généraux des deux sommes qu'il s'agit de multiplier entre elles, on aura :

$$\frac{1}{(N(n^2))^s (N(ax^2 + 2bxy + cy^2))^s} = \frac{1}{(N(ax'^2 + 2bx'y' + cy'^2))^s},$$

où l'on a posé $x' = nx$, $y' = ny$. Voyons quelle est la nature des systèmes x' , y' auxquels la nouvelle sommation doit se rapporter. Comme on a :

$$n^2(ax^2 + 2bxy + cy^2) = ax'^2 + 2bx'y' + cy'^2,$$

on voit d'abord, en ayant égard aux conditions que x , y , n sont supposés remplir, 1^o que pour chacun des systèmes en question, $ax'^2 + 2bx'y' + cy'^2$ est premier à \mathcal{A} , et 2^o que les entiers x' , y' satisfont à la double inégalité :

$$N(ax' + (b - \sqrt{D})y') < N(ax' + (b + \sqrt{D})y') \leq \sigma^2 N(ax' + (b - \sqrt{D})y')$$

de même forme que (3), et qui résulte de cette dernière en multipliant par $N(n)$. Il est facile de prouver réciproquement que tout système x' , y' qui satisfait à ces deux conditions, est en effet compris parmi ceux auxquels la nouvelle sommation doit s'étendre, et ne s'y présente qu'une fois. C'est à quoi l'on parvient, en assignant l'entier n et le système x , y , l'un et l'autre entièrement déterminés, dont la combinaison fournit le système donné x' , y' . Soit à cet effet $x' = nx$, $y' = ny$, où n désigne le plus grand diviseur commun primaire de x et y , qui sera complètement déterminé ainsi que les entiers x et y . Cela étant, il est évident que n est premier à \mathcal{A} , et l'on voit également sans difficulté que les entiers x et y , premiers entre eux, satisfont aussi aux deux autres conditions auxquelles les systèmes x , y sont assujettis. Cela est manifeste pour celle de ces conditions qui consiste en ce que $ax^2 + 2bxy + cy^2$ doit être premier à \mathcal{A} , et pour prouver que la double inégalité (3) a pareillement lieu, il suffit de diviser par $N(n)$ celle que nous avons écrite plus haut et à laquelle x' et y' sont supposés satisfaire.

Après avoir ainsi reconnu la nature des systèmes x' , y' que la nouvelle sommation doit embrasser, nous pouvons supprimer les accents des indéterminées x' et y' . L'équation qu'il s'agissait de transformer, deviendra ainsi :

$$(9) \quad 8 \sum \frac{1}{(N(n))^s} \cdot \sum \left[\frac{D}{n} \right] \frac{1}{(N(n))^s} = \sum \frac{1}{(N(ax^2 + 2bxy + cy^2))^s} + \dots,$$

où la double sommation indiquée dans le premier terme du second membre est supposée s'étendre aux valeurs simultanées x et y telles que $ax^2+2bxy+cy^2$ soit premier à \mathcal{A} , et satisfaisant en outre à la condition (3). Quant aux autres termes, comme ils sont de même nature que celui dont nous venons de parler, et résultent de ce dernier en accentuant les lettres a, b, c , nous continuerons à ne pas les écrire. Il s'agit maintenant de transformer l'équation que nous venons d'obtenir, de manière qu'elle exprime le nombre des formes non-équivalentes qui répondent au déterminant D . Ce sera là l'objet du paragraphe suivant.

Expression du nombre des classes au moyen d'une suite infinie double.

§. 18.

Pour parvenir au but que nous avons en vue, nous aurons à examiner ce que les différents termes de l'équation (9) du paragraphe précédent deviennent, lorsque la variable s que cette équation contient, converge vers sa limite qui est l'unité.

I. Occupons-nous d'abord du second membre, en nous bornant toujours à considérer la première des sommes dont ce membre se compose. Comme indépendamment de la double condition d'inégalité à laquelle x et y sont supposés satisfaire, ces indéterminées doivent être telles que la valeur du trinôme $ax^2+2bxy+cy^2$ soit première à \mathcal{A} , on conclut du §. 15, III que les valeurs simultanées de x et y que la sommation embrasse, peuvent être distribuées en systèmes de la forme:

$$(1) \quad x = v\mathcal{A} + a, \quad y = w\mathcal{A} + \gamma,$$

où v, w et a, γ désignent des entiers complexes, les deux premiers indéterminés et les deux derniers déterminés, et que le nombre de ces systèmes est toujours $N(\mathcal{A})\psi(\mathcal{A})$. La somme dont il s'agit se décompose ainsi en $N(\mathcal{A})\psi(\mathcal{A})$ sommes partielles, telles que la suivante:

$$(2) \quad \sum \frac{1}{(N(ax^2+2bxy+cy^2))^s},$$

où le signe sommatoire doit s'étendre à toutes les valeurs de x et y , données par les formules (1), et en outre telles que l'on ait:

$$(3) \quad N(ax+(b-\sqrt{D})y) < N(ax+(b+\sqrt{D})y) \leq \sigma^2 N(ax+(b-\sqrt{D})y).$$

Pour évaluer la somme partielle (2), soit z une variable positive, et proposons-nous de déterminer l'entier positif Z qui exprime combien de fois dans la somme dont il s'agit, l'expression $N(ax^2 + 2bxy + cy^2)$ obtient une valeur non-supérieure à z . On sent que Z est une fonction discontinue très compliquée de la variable z ; mais il ne s'agira pas d'obtenir cette fonction avec une exactitude absolue, et il suffira de connaître son expression-limite, c'est-à-dire une expression dont le rapport à Z converge vers l'unité, lorsque la variable z devient infinie. D'après ce qui précède, l'entier Z désigne le nombre des combinaisons v, w pour lesquelles on a, outre la condition (3), celle que nous allons écrire:

$$N(ax^2 + 2bxy + cy^2) \leq z,$$

ou ce qui revient au même, celle-ci:

$$(4) \quad N(ax + (b + \sqrt{D})y)N(ax + (b - \sqrt{D})y) \leq zN(a),$$

x et y étant supposés remplacés dans les conditions (3) et (4) par les expressions (1).

Observons maintenant que, comme il ne s'agit que d'obtenir le nombre des combinaisons v, w qui satisfont aux inégalités précédentes, nous pouvons remplacer les entiers v, w par d'autres indéterminées v', w' , entières ou non, mais tellement liées à v et w qu'à toute combinaison v, w réponde une combinaison unique v', w' , et réciproquement. Soit, pour abrégér, $z = \frac{1}{\xi}$, où ξ est supposé positif; il est facile de voir que nous remplirons la condition énoncée en posant les équations linéaires:

$$v' = \left(v + \frac{\alpha}{A}\right)\xi, \quad w' = \left(w + \frac{\gamma}{A}\right)\xi,$$

en vertu desquelles, ξ étant réel et v, w désignant des entiers complexes indéterminés, v' et w' exprimeront l'un et l'autre des nombres complexes, dont les deux parties sont les termes généraux de progressions arithmétiques réelles, ayant la quantité ξ pour raison commune. Au moyen de ces expressions les formules (1) que nous avons à substituer dans les conditions (3) et (4), deviennent:

$$x = \frac{v'A}{\xi}, \quad y = \frac{w'A}{\xi}.$$

Si maintenant l'on effectue la substitution dont il s'agit, et que l'on multiplie ensuite les inégalités (3) et (4) respectivement par $\frac{\xi^2}{N(A)}$ et $\frac{\xi^4}{N(A)^2}$, il viendra

simplement:

$$(5) \quad \begin{cases} N(av' + (b - \sqrt{D})w') < N(av' + (b + \sqrt{D})w') \leq \sigma^2 N(av' + (b - \sqrt{D})w'), \\ N(av' + (b + \sqrt{D})w')N(av' + (b - \sqrt{D})w') \leq N\left(\frac{a}{J^2}\right), \end{cases}$$

de sorte que le nombre Z qu'il s'agit de déterminer, coïncide maintenant avec celui des combinaisons v', w' qui satisfont à ces dernières inégalités, dans lesquelles v' et w' ont la signification indiquée plus haut.

Il faut maintenant remplacer les nombres complexes, contenus dans ces inégalités, par leurs éléments réels. Posons pour cela:

$$(6) \quad v' = x + x'i, \quad w' = y + y'i,$$

où les quatre quantités réelles x, x', y, y' sont les termes généraux d'autant de progressions arithmétiques, indéfiniment prolongées dans les deux sens et dont la raison commune est z . Posons encore:

$$(7) \quad a = \alpha + \alpha'i, \quad b = \beta + \beta'i, \quad \sqrt{D} = \delta + \delta'i,$$

$\alpha, \alpha', \beta, \beta', \delta, \delta'$ étant des constantes réelles, et soit enfin, pour abrégier:

$$(8) \quad \begin{cases} p = \alpha x - \alpha'x', & q = \beta y - \beta'y', & r = \delta y - \delta'y', \\ p' = \alpha'x + \alpha x', & q' = \beta'y + \beta y', & r' = \delta'y + \delta y'. \end{cases}$$

En substituant les expressions (6) et (7), les inégalités (5) prendront la forme:

$$(9) \quad \begin{cases} (p+q-r)^2 + (p'+q'-r')^2 < (p+q+r)^2 + (p'+q'+r')^2 \\ \leq \sigma^2((p+q-r)^2 + (p'+q'-r')^2), \\ ((p+q+r)^2 + (p'+q'+r')^2)((p+q-r)^2 + (p'+q'-r')^2) \leq N\left(\frac{a}{J^2}\right). \end{cases}$$

Il est maintenant facile de reconnaître que l'entier Z , lorsque la variable z dont il est fonction, devient infiniment petite, dépend de l'intégrale suivante:

$$(10) \quad \iiint \iiint dx dx' dy dy' = A.$$

dans laquelle les différentielles dx, dx', dy, dy' sont considérées comme positives, et qui est supposée s'étendre à toutes les valeurs des variables x, x', y, y' compatibles avec les conditions (9). En effet, si dans l'intégrale précédente l'on considère les quatre différentielles comme constantes et égales à z , tous les éléments de cette intégrale auront la valeur commune z^4 , de sorte que l'intégrale sera égale au produit de z^4 par le nombre des combinaisons x, x', y, y' qui satisfont aux conditions (9), et dans lesquelles les variables sont supposées

croître de la différence constante z . Or, ce dernier nombre étant précisément l'entier Z , on aura pour une valeur infiniment petite de z :

$$Zz^4 = A,$$

ou ce qui revient au même:

$$(11) \quad Z = Az,$$

z étant supposé infini. Il est encore facile de s'assurer qu'en même temps que le rapport des deux membres de cette dernière équation tend vers la limite 1, leur différence croît moins rapidement qu'une puissance de z , dont l'exposant constant serait tant soit peu supérieur à $\frac{3}{4}$, et généralement à $\frac{m-1}{m}$, s'il s'agissait d'une intégrale de l'ordre m^*).

Tout se réduit donc maintenant à obtenir la valeur A de l'intégrale (10). Pour y parvenir, on pourrait faire usage d'une substitution unique, mais le calcul devient beaucoup plus simple, si l'on emploie plusieurs substitutions successives. Observons que, l'ordre des intégrations étant arbitraire, nous pouvons considérer les intégrations relatives à x et x' comme devant être effectuées les premières, et que rien ne s'oppose alors à ce que nous remplacions les variables x et x' par de nouvelles variables t et t' , liées aux premières par des équations qui contiennent y et y' , pourvu que dans ces équations l'on traite y et y' comme des constantes. Posons donc:

$$t = p+q, \quad t' = p'+q',$$

p, q, p', q' désignant les expressions linéaires (8). Si l'on applique la formule connue qui sert à la transformation des intégrales doubles, on trouvera que le produit $dx dx'$ devra être remplacé par:

$$\frac{1}{a^2+a'^2} dt dt' = \frac{1}{N(a)} dt dt'.$$

*) Le principe dont nous faisons usage dans le texte, est évident et résulte immédiatement de la notion même d'une intégrale multiple, considérée comme une somme d'éléments infiniment petits. lorsque, comme il arrive ici, les variables ne doivent pas obtenir des valeurs infinies dans les intégrations qu'il s'agit d'effectuer; mais il est bon d'ajouter que si, l'intégrale elle-même restant toujours finie, cette dernière circonstance n'avait plus lieu, l'application du même principe pourrait conduire à des résultats entièrement erronés, ce dont il est facile de voir la raison, et comme on peut d'ailleurs s'en assurer par des exemples, en considérant une intégrale double exprimant une aire finie, comprise entre une courbe et son asymptote. Quant à l'assertion que nous venons d'avancer et d'après laquelle les variables x, x', y, y' ne sauraient être infinies dans notre cas, elle résulte trop simplement des conditions (9), pour qu'il soit nécessaire de nous y arrêter.

En substituant cette dernière expression dans l'intégrale et les nouvelles variables dans les conditions (9), qui définissent l'étendue des intégrations, on aura :

$$\begin{aligned} \iiint dt dt' dy dy' &= AN(a), \\ (t-r)^2 + (t'-r')^2 &< (t+r)^2 + (t'+r')^2 < a^2((t-r)^2 + (t'-r')^2), \\ ((t+r)^2 + (t'+r')^2)((t-r)^2 + (t'-r')^2) &< N\left(\frac{a}{J^2}\right), \end{aligned}$$

où nous avons supprimé les signes d'égalité qui accompagnaient ceux d'inégalité et qui sont désormais inutiles, les conditions précédentes se rapportant maintenant à des variables continues. Si en second lieu, t et t' étant considérés comme constants, nous remplaçons les variables y et y' à leur tour par de nouvelles variables r et r' , liées à y et y' par les deux dernières des formules (8), l'intégrale deviendra :

$$\iiint dt dt' dr dr' = AN(a\sqrt{D}),$$

les conditions qui en définissent l'étendue, étant toujours celles que nous venons d'écrire. Distribuons actuellement les quatre variables en ces deux groupes: $t, r; t', r'$, et remplaçons-les respectivement par ces deux nouveaux groupes: $x, x'; y, y'$, liés aux précédents par les équations :

$$x = t - r, \quad x' = t + r; \quad y = t' - r', \quad y' = t' + r',$$

en vertu desquelles il faudra mettre $\frac{1}{2} dx dx', \frac{1}{2} dy dy'$ respectivement à la place de $dt dr, dt' dr'$. L'intégrale et les conditions qui s'y rapportent, se changeront ainsi en :

$$\begin{aligned} \iiint dx dy dx' dy' &= 4AN(a\sqrt{D}), \\ x^2 + y^2 < x'^2 + y'^2 < a^2(x^2 + y^2), & (x^2 + y^2)(x'^2 + y'^2) < N\left(\frac{a}{J^2}\right). \end{aligned}$$

Remplaçons maintenant les variables de chacun des groupes x, y et x', y' par des coordonnées polaires, en posant :

$$x = \rho \cos \theta, \quad y = \rho \sin \theta; \quad x' = \rho' \cos \theta', \quad y' = \rho' \sin \theta',$$

où il importe de remarquer qu'indépendamment des conditions auxquelles les nouvelles variables doivent satisfaire en vertu des inégalités précédentes, il faudra regarder ρ comme positif et θ comme étant compris entre les limites 0 et 2π , pour qu'à une même combinaison x, y ne réponde pas plus d'une combinaison ρ, θ , et que ρ', θ' doivent être assujettis à la même limitation. Par l'intro-

duction de ces nouvelles variables, il viendra :

$$\iiint \varrho \varrho' d\varrho d\varrho' d\theta d\theta' = 4AN(a \mid D), \quad \varrho^2 < \varrho'^2 < \sigma^2 \varrho^2, \quad \varrho^2 \varrho'^2 < N\left(\frac{a}{J^2}\right).$$

Les conditions d'inégalité ne contenant pas les variables θ et θ' , les intégrations qui s'y rapportent, devront s'étendre depuis 0 jusqu'à 2π ; en effectuant ces deux intégrations et remplaçant en outre ϱ^2 , ϱ'^2 respectivement par ϱ , ϱ' , de sorte que ces nouvelles variables devront être considérées comme positives, on trouvera :

$$\iint d\varrho d\varrho' = \frac{4}{\pi^2} AN(a \mid \bar{D}), \quad \varrho < \varrho' < \sigma^2 \varrho, \quad \varrho \varrho' < N\left(\frac{a}{J^2}\right).$$

Si maintenant, ϱ étant regardé comme constant, nous remplaçons ϱ' par une nouvelle variable ν , déterminée par l'équation $\varrho' = \nu \varrho$, et qui en vertu de ce qui précède, doit être considérée comme positive, nous aurons d'abord :

$$\iint \varrho d\varrho d\nu = \frac{4}{\pi^2} AN(a \mid \bar{D}), \quad 1 < \nu < \sigma^2, \quad \varrho^2 < \frac{1}{\nu} N\left(\frac{a}{J^2}\right),$$

et par suite, en effectuant l'intégration relative à ϱ , et qui doit s'étendre depuis $\varrho^2 = 0$ jusqu'à $\varrho^2 = \frac{1}{\nu} N\left(\frac{a}{J^2}\right)$:

$$\int \frac{d\nu}{\nu} = \frac{8}{\pi^2} AN(J^2 \mid \bar{D}), \quad 1 < \nu < \sigma^2,$$

d'où l'on conclut enfin :

$$A = \frac{\pi^2 \log \sigma}{4N(J^2 \sqrt{D})}.$$

Après avoir ainsi déterminé le coefficient A , contenu dans l'équation (11), il sera facile de voir ce que la somme partielle (2) devient, lorsque l'exposant s converge vers l'unité, ou ce qui revient au même, lorsque la variable positive ϱ , supposée liée à s par l'équation $s = 1 + \varrho$, est considérée comme infiniment petite. En effet, comme la fonction Z qui exprime combien de fois dans la somme en question, l'expression $N(ax^2 + 2bxy + cy^2)$ obtient une valeur qui ne surpasse pas celle de z , est telle que les deux rapports :

$$\frac{Z}{Az}, \quad \frac{Z - Az}{z^{\gamma}},$$

où γ désigne une constante supérieure à la fraction $\frac{3}{4}$, convergent le premier vers une limite égale à l'unité, le second vers la limite zéro, lorsque la variable z devient plus grande que toute grandeur donnée, on conclut sur-le-champ, du

lemme démontré dans le §. 1 du Mémoire déjà plusieurs fois cité¹⁾, que pour une valeur infiniment petite de ϱ , la somme (2) prend cette forme très simple:

$$\frac{A}{\varrho} = \frac{\pi^2 \log \sigma}{4N(\mathcal{J}\sqrt{D})} \frac{1}{\varrho} \text{ *)}$$

Cette expression ne présente rien qui soit particulier à la somme partielle que nous avons considérée, ni même rien qui soit particulier à la somme totale dont cette somme partielle fait partie, puisqu'elle n'est fonction que du seul déterminant D , commun à toutes les formes quadratiques contenues dans le second membre de l'équation (9) du §. 17. On voit donc qu'il suffit de la multiplier par le nombre $N(\mathcal{J})\psi(\mathcal{J})$ des sommes partielles contenues dans une même somme totale, et par celui des formes qui constituent un système complet relativement au déterminant D , pour en conclure la valeur du second membre de l'équation dont il s'agit, lorsqu'on y considère ϱ comme infiniment petit. Il viendra ainsi:

$$(12) \quad H \frac{\pi^2 \psi(\mathcal{J}) \log \sigma}{4N(\mathcal{J}\sqrt{D})} \frac{1}{\varrho}$$

H désignant le nombre des classes qui dépendent au déterminant D .

II. Il s'agit maintenant de considérer le premier membre de l'équation citée. Ce membre pouvant se mettre sous la forme:

$$4\Sigma \frac{1}{(N(n))^s} \cdot 2\Sigma \left[\frac{D}{n} \right] \frac{1}{(N(n))^s},$$

occupons-nous d'abord du premier de ces deux facteurs. Comme la somme dont il s'agit, doit s'étendre à tous les entiers n , premiers à \mathcal{J} et en outre primaires, il est évident que nous pouvons faire abstraction de la dernière de ces deux conditions, pourvu qu'en même temps nous omettions le facteur 4. Les valeurs que n doit recevoir, peuvent se distribuer en systèmes de la forme

*) Quoique les deux propriétés dont nous venons de faire usage, ressortent l'une et l'autre avec évidence des considérations indiquées plus haut, il peut être bon de faire remarquer que la première de ces propriétés suffit à elle seule pour en tirer la conclusion que nous venons d'énoncer. C'est ce qui résulte d'une remarque déjà faite dans le Mémoire précédent, et d'après laquelle le lemme dont il s'agit, comporte plus d'étendue qu'il n'a été nécessaire de lui donner à l'endroit cité. Il est en effet facile de reconnaître que la vérité de ce lemme ne suppose qu'une seule condition, consistant en ce que la fonction, désignée par $f(t)$ dans son énoncé, doit être telle que l'on ait $\frac{f(t)}{t} = c$, lorsque t obtient une valeur infinie. Pour s'en assurer, on n'aura qu'à apporter une modification assez légère et qui se présente facilement, à la démonstration qui a été exposée dans le Mémoire précédent.

¹⁾ S. 415 und 416 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

$n = vJ + \alpha$, v et α désignant des entiers complexes, le premier indéterminé, le second déterminé pour chaque système, et devant être égalé successivement à tous ceux des termes d'un système de résidus pour le module J qui n'ont pas de diviseur commun avec ce module. Considérons la somme partielle, répondant à l'un quelconque de ces termes, et qui est:

$$\sum \frac{1}{(N(vJ + \alpha))^{1+q}}.$$

Pour en obtenir la valeur, soit z une variable positive et Z la fonction discontinue de z qui exprime le nombre des entiers v pour lesquels on a:

$$N(vJ + \alpha) \leq z.$$

Si nous posons, pour abrégér, $z = \frac{1}{\xi}$, ξ étant positif, et que nous remplacions v par une nouvelle indéterminée v' telle qu'on ait:

$$v' = \left(v + \frac{\alpha}{J} \right) \xi.$$

l'inégalité précédente se changera en celle-ci:

$$N(v') \leq \frac{1}{N(J)}.$$

et Z désignera alors le nombre des valeurs v' qui satisfont à cette condition. Or, en posant $v' = x + x'i$, x et x' seront évidemment les termes généraux de deux suites dont la première différence est constante et égale à ξ ; on voit donc, comme plus haut, que pour une valeur infinie de z , on aura $Z = Bz$, B désignant l'intégrale:

$$\iint dx dx', \quad x^2 + x'^2 < \frac{1}{N(J)}.$$

Mais cette intégrale étant évidemment égale à $\frac{\pi}{N(J)}$, on conclura du lemme déjà employé dans le numéro précédent que la somme partielle que nous considérons, se réduit simplement à $\frac{\pi}{N(J)} \frac{1}{q}$ lorsque la variable q est supposée devenir moindre que toute grandeur donnée: d'où il suit enfin:

$$(13) \quad 4 \sum \frac{1}{(N(n))^{1+q}} = \frac{\pi \psi(J)}{N(J)} \frac{1}{q}.$$

le signe sommatoire s'étendant, comme dans l'équation (9) du §. 17, à tous les entiers n premiers à J et en outre primaires.

III. Pour mettre enfin la seconde des deux sommes, rappelées au commencement du numéro précédent, sous la forme appropriée à notre but, il faut distinguer plusieurs cas différents que le déterminant D peut présenter. Observons pour cela que, si nous réunissons en un seul carré tous les facteurs doubles de D , nous pourrons toujours mettre cet entier sous la forme:

$$(14) \quad D = \chi Q V^2,$$

χ ayant l'une de ces quatre valeurs:

$$(15) \quad \chi = 1, \quad \chi = i, \quad \chi = 1+i, \quad \chi = i(1+i),$$

et Q ou $-Q$ désignant un produit de facteurs simples impairs et primaires, tous inégaux, sans exclure le cas où l'on aurait $Q = \pm 1$, qui ne peut toutefois avoir lieu qu'autant qu'on n'a pas $\chi = 1$, les déterminants carrés étant toujours exclus. Nous ajouterons que si les entiers χ , Q , V doivent être tels que nous venons de les définir, ils seront complètement déterminés pour tout déterminant donné, si ce n'est que Q , V^2 peuvent être simultanément remplacés par $-Q$, $(V)^2$.

Cela posé, nous allons transformer l'expression $\left[\frac{D}{n}\right]$ au moyen des équations (e) et (f) du §. 8. On a d'abord évidemment en vertu des équations citées:

$$\left[\frac{D}{n}\right] = \left[\frac{\chi Q V^2}{n}\right] = \left[\frac{\chi}{n}\right] \left[\frac{Q}{n}\right] = \left[\frac{\chi}{n}\right] \left[\frac{n}{Q}\right].$$

Pour transformer le facteur $\left[\frac{\chi}{n}\right]$, il devient nécessaire d'introduire explicitement les deux entiers réels contenus dans n ; posons donc $n = \lambda + \nu i$, λ et ν étant respectivement des formes $4k+1$, $2k$. Il viendra alors suivant les quatre cas déjà distingués (15), et en ayant égard aux deux premières des équations (f) citées:

$$\begin{aligned} \left[\frac{\chi}{n}\right] &= 1, & \left[\frac{\chi}{n}\right] &= (-1)^{\frac{1}{2}(\lambda^2 + \nu^2 - 1)}, \\ \left[\frac{\chi}{n}\right] &= (-1)^{\frac{1}{2}((\lambda + \nu)^2 - 1)}, & \left[\frac{\chi}{n}\right] &= (-1)^{\frac{1}{2}(\lambda^2 + \nu^2 - 1) + \frac{1}{2}((\lambda + \nu)^2 - 1)}. \end{aligned}$$

Pour réunir ces quatre expressions en une seule formule, nous poserons $\delta = \pm 1$, $\varepsilon = \pm 1$, les signes ambigus étant choisis suivant les quatre cas que χ peut présenter en vertu des équations (15), comme il suit:

$$(16) \quad \delta = 1, \quad \varepsilon = 1; \quad \delta = -1, \quad \varepsilon = 1; \quad \delta = 1, \quad \varepsilon = -1; \quad \delta = -1, \quad \varepsilon = -1.$$

Cette convention admise, nous aurons pour tous les cas:

$$\left[\frac{\chi}{n}\right] = \delta^{\frac{1}{2}(\lambda^2 + \nu^2 - 1)} \varepsilon^{\frac{1}{2}((\lambda + \nu)^2 - 1)}.$$

Au moyen de cette dernière expression et de celles déjà obtenues, le facteur du premier membre de l'équation (9) du §. 17. qu'il s'agissait de transformer, prendra la forme:

$$(17) \quad 2\Sigma \left[\frac{D}{n} \right] \frac{1}{(N(n))^{1+\rho}} = 2\Sigma \delta^{\frac{1}{4}(\lambda^2+\nu^2-1)} \varepsilon^{\frac{1}{4}(\lambda+\nu)^2-1} \left[\frac{\lambda+\nu i}{Q} \right] \frac{1}{(\lambda^2+\nu^2)^{1+\rho}}.$$

IV. Si maintenant nous substituons les expressions (12), (13) et (17) dans l'équation citée, et que nous effaçons le facteur $\frac{1}{Q}$ et les autres facteurs communs aux deux membres, l'équation dont il s'agit, prendra la forme:

$$(18) \quad H = \frac{8N(\overline{D})}{\pi \log \sigma} \Sigma \delta^{\frac{1}{4}(\lambda^2+\nu^2-1)} \varepsilon^{\frac{1}{4}(\lambda+\nu)^2-1} \left[\frac{\lambda+\nu i}{Q} \right] \frac{1}{(\lambda^2+\nu^2)^{1+\rho}}.$$

Telle est la suite infinie double qui exprime le nombre des classes pour un déterminant quelconque non-carré D , et dans laquelle nous avons conservé la quantité infiniment petite ρ , qui ne doit être annulée qu'après que l'on aura fixé l'ordre dans lequel les termes de la double somme doivent se suivre, pour que cette somme soit en effet la limite de celle qui répond à une valeur infiniment petite de la variable positive ρ . La signification des lettres qui entrent dans l'équation, a été fixée dans ce qui précède, et l'on devra se rappeler que la double sommation doit s'étendre à tous les couples d'entiers réels λ et ν , respectivement des formes $4k+1$, $2k$, et tels que l'entier complexe correspondant $\lambda+\nu i$ soit premier à D .

Pour effectuer la double sommation, il faudra d'abord transformer le facteur $\left[\frac{\lambda+\nu i}{Q} \right]$ au moyen de l'équation (h) du §. 8, et remplacer ensuite les nouveaux symboles ainsi introduits par une suite finie de sinus ou de cosinus, en se servant pour cet objet des formules connues dues à M. GAUSS. Après ces deux substitutions, l'une des deux sommations pourra être exécutée au moyen d'une suite trigonométrique, dont la somme a été donnée par EULER, et la suite infinie double, réduite par-là à une série simple, se décomposera alors en plusieurs séries partielles qui rentrent dans celles par lesquelles ABEL et M. JACOBI ont développé les fonctions trigonométriques de l'amplitude d'une fonction elliptique de première espèce. Mais si avec le secours des formules dont les illustres géomètres que nous venons de citer, ont enrichi l'Analyse, la sommation en elle-même ne présente pas de difficulté réelle et n'exige que peu d'espace, il n'en est pas de même de la discussion à laquelle il faut soumettre

le résultat qui s'en déduit, pour en reconnaître la véritable nature. Comme le résultat dont il s'agit, se trouve dépendre de la division en parties égales de la fonction elliptique complète de première espèce, pour le cas où le module a la valeur $\sqrt{\frac{1}{2}}$, et où le nombre de ces parties égales est un entier complexe, et que la théorie des équations algébriques qui se rapportent à une telle division, n'a été qu'ébauchée jusqu'à présent*), il sera nécessaire d'entrer à cet égard dans de nouveaux développements dont l'étendue excéderait de beaucoup les bornes que nous avons dû imposer à cette première partie de notre travail. C'est pourquoi et comme nous en avons déjà averti, nous réserverons ces détails pour la seconde partie, et nous terminerons celle-ci par l'examen des deux cas particuliers, déjà mentionnés dans le préambule du présent Mémoire.

Examen de deux cas particuliers.

§. 19.

Les deux cas qu'il s'agit de considérer, sont ceux où le déterminant D est un entier réel ou le produit d'un tel entier par i . Comme en vertu de l'équation (18) du paragraphe précédent, le nombre des classes est évidemment le même pour deux déterminants opposés, nous pourrions toujours considérer comme positif, l'entier dont il vient d'être question.

I. Soit en premier lieu D un entier positif non-carré, et soit S^2 le plus grand carré réel qui divise D . Nous aurons alors l'un de ces deux cas :

$$(1) \quad D = PS^2, \quad D = 2PS^2,$$

P désignant un produit de nombres premiers positifs, impairs et tous inégaux, produit qui peut d'ailleurs se réduire à l'unité dans le second cas. Comme, en considérant P comme complexe, cet entier ou son opposé est primaire et n'a que des facteurs simples inégaux, il suffit de mettre la seconde des équations (1) sous la forme $D = iP((1-i)S)^2$, pour reconnaître que les équations (14), (15) et (16) du §. 18, qui se rapportent à un déterminant quelconque, donnent relativement au cas particulier qui nous occupe, $Q = P$, $\varepsilon = 1$, $\delta = \pm 1$, où il faut choisir le signe supérieur ou le signe inférieur dans la dernière de ces équations, selon que D présente le premier ou le second des deux cas (1). En substituant

*) Voir un Mémoire d'ABEL, inséré dans le Journal de CRELLE, Tome III, p. 160¹⁾.

¹⁾ Oeuvres complètes de N. H. Abel, Édition de 1839, T. I, p. 221; Édition de 1881, T. I, p. 352. K.

ces valeurs dans l'expression générale de H , et remplaçant en même temps σ par sa valeur, donnée par la formule (3) du §. 14, ainsi que $\left[\frac{\lambda + \nu i}{P}\right]$ par l'expression équivalente, fournie par la première des équations (g) du §. 8, il viendra :

$$(2) \quad H = \frac{8D}{\pi x \log(\tau + \nu) D} \sum \delta^{\frac{1}{2}(\lambda^2 + \nu^2 - 1)} \left(\frac{\lambda^2 + \nu^2}{P}\right) \frac{1}{(\lambda^2 + \nu^2)^{1+\varepsilon}},$$

de sorte que la somme double ne contient plus l'entier complexe $\lambda + \nu i$, mais seulement sa norme $\lambda^2 + \nu^2$. Il est vrai que cet entier semble y entrer encore implicitement par la condition que $\lambda + \nu i$ doit être premier à D ; mais ce dernier entier étant réel, on voit que la condition dont il s'agit, revient à celle que D et $\lambda^2 + \nu^2$ doivent être sans diviseur commun.

II. Considérons en second lieu un déterminant de la forme $D = D'i$, D' étant un entier positif qu'il faudra seulement supposer tel que $2D'$ ne soit pas un carré, sans quoi D serait lui-même un carré. Si nous désignons par S'^2 le plus grand carré réel qui divise $2D'$, nous aurons l'une ou l'autre de ces deux équations :

$$(3) \quad 2D' = P'S'^2, \quad 2D' = 2P'S'^2,$$

dans lesquelles P' est un produit de nombres premiers positifs, impairs et inégaux, S' étant pair dans la première de ces deux équations. Ces équations donnent respectivement celles-ci :

$$D = P'((1+i)\frac{1}{2}S')^2, \quad D = P'iS'^2,$$

qu'il suffit de comparer aux équations déjà citées du §. 18, pour voir que nous avons $Q = P'$, $\varepsilon = 1$, $\delta = \pm 1$, le signe supérieur ou le signe inférieur devant être choisi, selon que $2D'$ présente le premier ou le second des deux cas (3). Au moyen de ces valeurs et par des transformations analogues à celles que nous avons opérées dans le numéro précédent, l'on trouvera :

$$(4) \quad H = \frac{8D'}{\pi x \log(\tau + \nu) \sqrt{2D'}} \sum \delta^{\frac{1}{2}(\lambda^2 + \nu^2 - 1)} \left(\frac{\lambda^2 + \nu^2}{P'}\right) \frac{1}{(\lambda^2 + \nu^2)^{1+\varepsilon}},$$

x , τ , ν ayant la même signification que dans l'équation (4) du §. 14, et la double sommation devant s'étendre à tous les couples d'entiers réels λ , ν , respectivement compris dans les formes $4k+1$, $2k$, et tels que $\lambda^2 + \nu^2$ soit premier à D' .

III. Nous allons maintenant faire voir que les sommes doubles (2) et (4) peuvent être remplacées chacune par un produit de deux séries simples. La

transformation qu'il s'agit d'effectuer, n'est qu'une application très particulière de certaines équations générales dont nous avons eu à faire usage dans le Mémoire précédent (§. 6. V.)¹⁾; mais, pour mieux faire sentir le principe sur lequel cette transformation repose, il nous paraît préférable de la rattacher à un théorème arithmétique très simple et susceptible d'une démonstration tout élémentaire. Voici en quoi consiste ce théorème:

...*m* désignant un entier positif et impair donné, le nombre des solutions de l'équation $m = x^2 + y^2$, dans laquelle *x* et *y* sont des entiers réels indéterminés, est égal au quadruple excès du nombre des diviseurs (positifs) de *m*, qui sont compris dans la forme $4k+1$, sur celui de ces diviseurs qui ont la forme $4k+3$.²⁾

Comme les entiers *x* et *y* qui satisfont à l'équation précédente, sont toujours l'un pair, l'autre impair, on voit que si l'on considère l'un de ces entiers, le second par exemple, comme devant être pair, le nombre des solutions se réduira de moitié, et l'on voit également que si l'on suppose en outre *x*, pris avec son signe, de la forme $4k+1$, le nombre des solutions éprouvera une seconde réduction de même étendue, et deviendra simplement égal à l'excès défini dans l'énoncé, puisqu'à une même valeur de *y* répondent toujours deux valeurs opposées de *x*, qui sont l'une de la forme $4k+1$, l'autre de la forme $4k+3$. Au moyen de ce résultat, il est facile de former l'équation générale que nous allons écrire:

$$\Sigma F(x^2+y^2) = \Sigma (-1)^{\frac{1}{2}(n-1)} F(nm'),$$

et dans laquelle la double sommation, indiquée dans le premier membre, doit s'étendre à tous les entiers positifs ou négatifs *x* et *y*, respectivement compris dans les formes $4k+1$, $2k$, tandis que celle du second membre est supposée embrasser tous les entiers impairs et positifs *n* et *n'*. D'après la manière dont cette équation subsiste, il est encore évident qu'elle ne cessera pas d'avoir lieu, si aux conditions énoncées nous ajoutons celles que $x^2 + y^2$ soit premier à un entier réel donné *K*, et qu'il en soit de même du produit *nm'*, ces nouvelles conditions n'ayant d'autre effet que de supprimer les mêmes termes de part et d'autre. Ainsi restreintes, les indéterminées *x* et *y* auront la même signification

¹⁾ S. 456 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

²⁾ Voyez pour la démonstration de ce théorème, dû à M. JACOBI, le Tome XII du Journal de CRELLE, p. 167, ou le Mémoire cité, §. 7. ²⁾

²⁾ S. 463 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

que celles désignées par λ et ν dans les sommes (2) et (4), en supposant respectivement $K = D$ ou $K = D'$, tandis que n et n' devront être respectivement supposés premiers à D ou à D' . Cela posé, si dans les deux sommes (2) et (4) nous remplaçons l'exposant de δ , par le produit :

$$\frac{1}{4}(\lambda^2 + \nu^2 - 1) \cdot \frac{1}{2}(\lambda^2 + \nu^2 + 1) = \frac{1}{8}((\lambda^2 + \nu^2)^2 - 1),$$

ce qui est permis, le facteur ajouté étant impair, il suffira de supposer la fonction arbitraire $F(z)$ de la forme :

$$\delta^{\frac{1}{8}(z^2-1)} \left(\frac{z}{P} \right) \frac{1}{z^{1+\varphi}}.$$

pour conclure de l'équation en question que la somme double (2) est équivalente à celle-ci :

$$\Sigma (-1)^{\frac{1}{2}(n-1)} \delta^{\frac{1}{8}((nn')^2-1)} \left(\frac{nn'}{P} \right) \frac{1}{(nn')^{1+\varphi}},$$

où le signe Σ se rapporte à tous les entiers positifs n et n' , impairs et premiers à D . Observons maintenant que, l'exposant de δ étant toujours pair ou impair en même temps que le nombre $\frac{1}{8}(n^2-1) + \frac{1}{8}(n'^2-1)$, comme nous avons déjà eu occasion de le remarquer dans le § 8, nous pouvons le remplacer par ce dernier. Par cette substitution, le terme général de la somme précédente se changera en un produit de deux facteurs qui ne contiennent chacun qu'un seul des entiers n et n' , de sorte que la somme elle-même prendra la forme d'un produit de deux séries simples. On obtient ainsi et en substituant dans l'équation (2), celle que nous allons écrire :

$$(2') \quad H = \frac{8D}{\pi \kappa \log(\tau + \nu \sqrt{D})} \Sigma \delta^{\frac{1}{8}(n^2-1)} \left(\frac{n}{P} \right) \frac{1}{n} \cdot \Sigma (-1)^{\frac{1}{2}(n-1)} \delta^{\frac{1}{8}(n^2-1)} \left(\frac{n}{P} \right) \frac{1}{n},$$

chacune des deux sommations indiquées s'étendant à tous les entiers positifs n , impairs et premiers à D . Pour plus de simplicité, nous avons remplacé n' par n , ce qui est permis, ces deux lettres ayant la même signification et ne se trouvant plus maintenant mêlées dans une même sommation. Nous avons en outre réduit à zéro la variable infiniment petite φ , les sommes précédentes étant en effet les limites de celles où l'on aurait conservé la quantité φ , pourvu que dans ces sommes l'on considère les entiers n comme formant une suite croissante, comme il est facile de s'en assurer, et comme on l'a d'ailleurs prouvé, en établissant les résultats qu'il sera nécessaire de rappeler dans le numéro suivant.

L'équation (4) étant soumise aux mêmes transformations, se changera en celle-ci :

$$(4') \quad H = \frac{8D'}{\pi x \log(\tau + v\sqrt{2D'})} \sum \delta^{\frac{1}{2}(n^2-1)} \left(\frac{n}{P'}\right) \frac{1}{n} \cdot \Sigma (-1)^{\frac{1}{2}(n-1)} \delta^{\frac{1}{2}(n^2-1)} \left(\frac{n}{P'}\right) \frac{1}{n}.$$

IV. Il faut maintenant rappeler les résultats qui se rapportent aux formes quadratiques à coefficients réels, pour les comparer à ceux que nous venons d'établir. C'est ce que nous allons faire, en choisissant les notations de manière à faciliter la comparaison dont il s'agit. Dans le Mémoire précédent (§. 6, éq. 23)¹⁾, on a démontré que relativement à un déterminant positif non-carré D , le nombre des classes que nous désignerons par h_1 , est donné par l'équation :

$$(5) \quad h_1 = \frac{2\sqrt{D}}{\log(\tau + v\sqrt{D})} \sum \theta^{\frac{1}{2}(n-1)} \delta^{\frac{1}{2}(n^2-1)} \left(\frac{n}{P}\right) \frac{1}{n}.$$

Dans cette équation la signification des lettres τ, v, δ, P et n est la même que dans les équations précédentes (1), (2) et (2'), et la sommation a la même étendue que dans la dernière de ces équations. Quant à la lettre θ , elle désigne l'unité positive ou négative, selon que P est de la forme $4k+1$ ou $4k+3$. Si nous considérons en second lieu le déterminant opposé $-D$, et que nous dénotions par h_2 le nombre des classes qui y répondent, il résulte de l'équation (19)²⁾ du paragraphe déjà cité, qu'on aura :

$$(6) \quad h_2 = \frac{2\sqrt{D}}{\pi} \sum (-\theta)^{\frac{1}{2}(n-1)} \delta^{\frac{1}{2}(n^2-1)} \left(\frac{n}{P}\right) \frac{1}{n},$$

la signification de toutes les lettres et l'étendue de la sommation restant toujours les mêmes. Or, θ étant toujours de la forme ± 1 , on voit que les deux séries contenues dans les équations (5) et (6), coïncident avec celles de l'équation (2'), de sorte qu'en divisant cette dernière par le produit des deux autres (5) et (6), on trouvera ce résultat très simple :

$$H = \frac{2}{x} h_1 h_2.$$

L'autre cas qui est celui d'un déterminant de la forme $D'i$, conduit à un résultat analogue; il suffit pour l'obtenir, de remplacer dans ce qui précède, les équations (5) et (6), par celles qui expriment les nombres h_1 et h_2 des classes

¹⁾ S. 456 dieser Ausgabe von G. Lejeune Dirichlet's Werken.

²⁾ S. 451 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K
G. Lejeune Dirichlet's Werke.

réelles répondant aux déterminants $2D'$ et $-2D'$. On trouve alors:

$$H = \frac{1}{x} h_1 h_2.$$

Nous avons donc ces deux théorèmes très remarquables:

„ D désignant un entier positif non-carré, soit H le nombre de classes dans lesquelles se distribuent les formes à coefficients complexes et au déterminant D , soient encore h_1 et h_2 les nombres de classes pour les formes à coefficients réels, répondant respectivement aux deux déterminants D et $-D$; toutes ces formes étant supposées telles que les coefficients extrêmes et le double coefficient moyen ne présentent pas de diviseur commun. Cela étant, on aura toujours:

$$H = 2h_1 h_2 \quad \text{ou} \quad H = h_1 h_2,$$

selon que l'équation indéterminée $t^2 - Du^2 = -1$ admettra des solutions réelles ou non.“

„ D désignant un entier positif dont le double ne soit pas un carré, si l'on suppose que les lettres H , h_1 , h_2 , en conservant une signification analogue à celle de l'énoncé précédent, se rapportent maintenant aux déterminants Di , $2D$, $-2D$, on aura:

$$H = h_1 h_2 \quad \text{ou} \quad 2H = h_1 h_2,$$

selon que l'équation $t^2 - 2Du^2 = -1$ admettra des solutions réelles ou non.“*)

Quoique les théorèmes précédents ne contiennent aucun élément qui ne soit relatif aux nombres entiers, il paraît difficile de les établir par des considérations purement arithmétiques, tandis que la méthode mixte dont nous venons de faire usage, et qui est fondée en partie sur l'emploi de quantités variant par degrés insensibles, nous y a conduit de la manière la plus naturelle et, pour ainsi dire, sans effort.

*) On suppose tacitement dans ces énoncés, comme on le fait ordinairement, que pour un déterminant négatif on n'admette que des formes réelles dont les coefficients extrêmes soient positifs. Si l'on n'adoptait pas cet usage, le nombre h_2 aurait une valeur double de celle que nous lui supposons, et les deux énoncés seraient à modifier en conséquence.

SUR LA THÉORIE DES NOMBRES.

PAR

G. LEJEUNE DIRICHLET.

Comptes rendus hebdomadaires des séances de l'Académie des Sciences, Tome X, p. 285 — 288.

SUR LA THÉORIE DES NOMBRES.

[Extrait d'une lettre adressée à M. LIOUVILLE.]

En voyant dans votre Journal l'élégante traduction que M. TERQUEM a bien voulu faire de mon *Mémoire sur la progression arithmétique**), j'ai eu l'idée d'étendre la même analyse aux formes quadratiques. En combinant cette analyse avec les considérations ingénieuses que M. GAUSS développe dans les derniers numéros de sa cinquième section, on prouve non seulement que toute forme quadratique renferme une infinité de nombres premiers, mais encore qu'elle en contient qui soient d'une forme linéaire quelconque compatible avec la forme quadratique donnée.

Je me suis aussi beaucoup occupé dans ces derniers temps à étendre aux formes quadratiques à coefficients et indéterminées complexes, c'est-à-dire de la forme $t+u\sqrt{-1}$, les théorèmes qui ont lieu dans les cas ordinaires des entiers réels. Si l'on cherche en particulier à obtenir le nombre des formes quadratiques différentes qui existent dans cette hypothèse pour un déterminant donné, on arrive à ce résultat assez remarquable, que le nombre dont il s'agit dépend de la division de la lemniscate, de même que dans le cas des formes réelles et à déterminant positif, il se rattache à la section du cercle. Ce qui m'a surtout fait plaisir dans ce travail, c'est le parti qu'on y tire de considérations géométriques et particulièrement de la théorie des propriétés perspectives des figures. Au moyen de cet auxiliaire, la question qui d'abord, et considérée d'une manière purement analytique, paraît extrêmement compliquée, devient presque aussi simple que lorsqu'il s'agit de déterminants réels.

*) Tome IV du Journal de LIOUVILLE, page 395¹⁾.

¹⁾ Bd. II dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

Les recherches dont je viens de vous indiquer l'objet, m'ont conduit à un théorème remarquable par sa simplicité et qui ne paraît pas sans importance pour la théorie des équations indéterminées des degrés supérieurs au second, matière encore très peu cultivée. Voici en quoi consiste ce théorème:

„Si l'équation:

$$(1) \quad s^n + a s^{n-1} + \dots + g s + h = 0,$$

à coefficients entiers, n'a pas de diviseur rationnel, et si parmi ses racines:

$$\alpha, \beta, \dots, \omega$$

il y en a au moins une qui soit réelle, je dis que l'équation indéterminée:

$$(2) \quad F(x, y, \dots, z) = g(\alpha)g(\beta)\dots g(\omega) = 1,$$

où l'on a posé pour abrégier:

$$g(\alpha) = x + \alpha y + \dots + \alpha^{n-1} z,$$

a toujours une infinité de solutions entières.“

Pour établir ce théorème, il faut d'abord faire voir qu'il existe au moins un entier m tel que l'équation:

$$(3) \quad F(x, y, \dots, z) = m$$

ait une infinité de solutions. C'est à quoi l'on peut parvenir par différents moyens. Dans le cas du second degré, la chose, qui pour ce cas n'est pas nouvelle, résulte immédiatement des propriétés des fractions continues.

L'équation (3) ayant une infinité de solutions, il en existera deux telles que l'on ait:

$$F(x, y, \dots, z) = m, \quad F(x', y', \dots, z') = m,$$

et en même temps:

$$(4) \quad x \equiv x', \quad y \equiv y', \quad \dots, \quad z \equiv z' \pmod{m}.$$

Cela posé, si nous considérons la fraction:

$$\frac{x' + \alpha y' + \dots + \alpha^{n-1} z'}{x + \alpha y + \dots + \alpha^{n-1} z},$$

on pourra évidemment, en multipliant par:

$$g(\beta) \dots g(\omega),$$

lui donner la forme:

$$\frac{X + \alpha Y + \dots + \alpha^{n-1} Z}{m},$$

où X, Y, \dots, Z sont des fonctions entières et à coefficients entiers de :

$$x, y, \dots, z, \quad x', y', \dots, z'.$$

Je dis maintenant que X, Y, \dots, Z sont des multiples de m . Pour le faire voir, admettons pour un instant que dans ces expressions :

$$x', y', \dots, z'$$

soient changés en :

$$x, y, \dots, z,$$

changement par lequel X, Y, \dots, Z resteront, en vertu des congruences (4), congrus à eux-mêmes. Par le changement dont il s'agit :

$$X + aY + \dots + a^{n-1}Z$$

doit devenir égal à m , ce qui ne peut arriver [l'équation (1) n'ayant pas de diviseurs rationnels] qu'autant que :

$$X, Y, \dots, Z$$

deviennent respectivement :

$$m, 0, \dots, 0.$$

Done X, Y, \dots, Z sont divisibles par m , et la fraction considérée plus haut est :

$$\xi + a\eta + \dots + a^{n-1}\zeta,$$

ξ, η, \dots, ζ étant des entiers; d'où l'on conclut :

$$F(\xi, \eta, \dots, \zeta) = 1,$$

solution qui en fournira une infinité d'autres.

Parmi les conséquences nombreuses qu'on peut tirer de ce théorème, il y en a une qui se présente pour ainsi dire d'elle-même; elle consiste en ce que les fonctions que LAGRANGE a d'abord considérées dans les *Mémoires de Berlin*, plus tard dans les *Additions à l'Algèbre* d'EULER, et qui se reproduisent par multiplication, si elles peuvent obtenir une certaine valeur, sont dès lors susceptibles de la même valeur pour une infinité de systèmes de valeurs des indéterminées x, y, \dots, z , en supposant toutefois que l'équation algébrique d'où ces fonctions tirent leur origine satisfasse aux conditions ci-dessus énoncées.

EINIGE RESULTATE VON UNTERSUCHUNGEN
ÜBER EINE CLASSE HOMOGENER FUNCTIONEN
DES DRITTEN UND DER HÖHEREN GRADE.

VON

G. LEJEUNE DIRICHLET.

Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1841, S. 280—285.

EINIGE RESULTATE VON UNTERSUCHUNGEN ÜBER EINE CLASSE HOMOGENER FUNCTIONEN DES DRITTEN UND DER HÖHEREN GRADE.

[Mitgetheilt in der Sitzung der physikalisch-mathematischen Classe
der Akademie der Wissenschaften am 11. October 1841.]

Die homogenen Functionen mit ganzzahligen Coefficienten, auf welche sich diese Untersuchungen beziehen, sind diejenigen besonderen Functionen jedes Grades, welche eine ihrem Grade gleiche Anzahl von unbestimmten ganzen Zahlen enthalten und zugleich in lineare Factoren mit irrationalen Coefficienten zerlegt werden können. Für den zweiten Grad fallen dieselben mit den so vielfach behandelten binären quadratischen Formen zusammen, und wie die Theorie dieser Formen einen der fruchtbarsten Theile der Arithmetik bildet, so kommen auch den analogen Ausdrücken von höherem Grade eine Menge der interessantesten Eigenschaften zu, deren Erforschung nicht nur der Theorie der Zahlen sondern auch anderen damit zusammenhängenden Disciplinen bedeutende Erweiterungen zu versprechen scheint. Von den zahlreichen Untersuchungen, zu welchen dieser Gegenstand Veranlassung giebt, betrifft die der Classe gemachte Mittheilung nur die Aufgabe:

„Alle Darstellungen einer gegebenen Zahl durch eine gegebene Function der genannten Art aufzufinden, oder sich doch zu überzeugen, dass die gegebene Zahl einer solchen Darstellung nicht fähig ist.“

Um die Betrachtungen, auf welchen die Lösung der eben ausgesprochenen Frage beruht, in das gehörige Licht zu setzen, wird es zweckmässig sein, dieselben zunächst auf den zweiten Grad anzuwenden, obgleich die Aufgabe für diesen Fall längst durch andere Methoden ihre vollständige Erledigung gefunden hat.

Für diesen Fall verlangt die Aufgabe, dass man alle Auflösungen der unbestimmten Gleichung:

$$(1) \quad ax^2 + 2bxy + cy^2 = m$$

darstelle, in welcher:

$$b^2 - ac = D$$

als positiv und keinem Quadrate gleich vorausgesetzt werden kann, da sonst die Frage gar keine Schwierigkeit darbietet. Die Methode, welche wir anzuwenden versuchen wollen, macht die Lösung dieses Problems von der Kenntniss irgend zweier Werthe abhängig, welche der bekanntlich immer möglichen Gleichung:

$$(2) \quad t^2 - Du^2 = 1$$

genügen. Sind:

$$T, U$$

zwei solche Werthe (die wir beide positiv voraussetzen können), und hätte man andererseits irgend eine Auflösung:

$$(X, Y)$$

der Gleichung (1), so würde man, nach einer von EULER gemachten Bemerkung, unzählige neue Auflösungen daraus ableiten können, welche durch die Formel:

$$(3) \quad ax + (b + \sqrt{D})y = \pm (aX + [b + \sqrt{D}]Y)(T + U\sqrt{D})^n$$

bestimmt werden, in welcher n irgend eine positive oder negative ganze Zahl bezeichnet, und nach geschehener Entwicklung die rationalen Theile und die Coefficienten von \sqrt{D} auf beiden Seiten besonders gleich zu setzen sind. Wie wichtig die von EULER gemachte Bemerkung auch sei, so begründet dieselbe doch noch keineswegs eine vollständige Zurückführung der Gleichung (1) auf die Gleichung (2), da dieselbe kein Mittel an die Hand giebt, eine erste Auflösung:

$$(X, Y)$$

zu finden, und andererseits, wie LAGRANGE gezeigt hat, der Ausdruck (3) nicht nothwendig alle Auflösungen der Gleichung (1) zu enthalten braucht, selbst wenn man für:

$$T, U$$

die kleinsten der Gleichung (2) genügenden Werthe wählt.

Um nun die oben verlangte vollständige Zurückführung zu bewerkstelligen, bemerke man, dass die in (3) enthaltenen Auflösungen eine Gruppe bilden,

welche dieselben Auflösungen zu enthalten fortfahren wird, wenn man statt der Auflösung (X, Y) irgend eine der daraus ableitbaren einführt. Es folgt hieraus, dass die Gesamtheit aller Auflösungen der Gleichung (1) in Gruppen dieser Art vertheilt werden kann, und dass es zur vollständigen Lösung unserer Aufgabe nur darauf ankommen wird, aus jeder Gruppe eine Auflösung zu kennen, da alsdann die ganze Gruppe selbst durch (3) gegeben sein wird. Nun ist aber aus (3) klar, dass in jeder Gruppe der Ausdruck:

$$ax + (b + \sqrt{D})y$$

nothwendig einmal und nur einmal einen Werth annimmt, der zwischen die beiden Grenzen:

$$\sigma \quad \text{und} \quad \sigma(T + U\sqrt{D})$$

mit Ausschluss von einer derselben fällt, wenn σ einen beliebigen positiven oder negativen Werth bezeichnet. Nimmt man z. B. σ positiv, so giebt es also in jeder Gruppe eine und nur eine Auflösung von solcher Beschaffenheit, dass:

$$(4) \quad \sigma < ax + (b + \sqrt{D})y \leq \sigma(T + U\sqrt{D}).$$

Mit diesem Resultate ist nun die Frage sogleich erledigt, da man leicht durch eine endliche Anzahl von Versuchen alle den Ungleichheiten (4) genügenden Auflösungen der Gleichung (1) finden oder doch sich überzeugen kann, dass keine solche existirt. Man sieht die Möglichkeit hiervon sogleich, wenn man der Sache eine geometrische Einkleidung giebt. Als Gleichung einer auf rechtwinklige Coordinaten bezogenen Curve betrachtet, stellt (1) eine Hyperbel dar, von welcher nur ein endlicher Bogen den Bedingungen (4) genügt, so dass man also in der That leicht alle innerhalb dieses Bogens liegenden Punkte finden kann, deren Coordinaten ganze Zahlen sind. Jeder dieser Punkte bestimmt dann eine Gruppe von Auflösungen der Gleichung (1), und falls sich keiner findet, ist die Unmöglichkeit dieser Gleichung dargethan.

Wie man sieht, ist der Erfolg des eben beschriebenen Verfahrens von der Wahl der Auflösung (T, U) , welche dabei als Ausgangspunkt dient, ganz unabhängig. Die Rechnung wird jedoch am kürzesten, wenn diese Auflösung die in den kleinsten Zahlen ausgedrückte ist, aus welcher bekanntlich alle übrigen durch Potenziren erhalten werden können. Wählt man eine dieser abgeleiteten, so hat dies keinen anderen Uebelstand, als dass die Anzahl der Gruppen im Endresultat dadurch vergrößert wird.

Indem wir zum dritten Grade übergehen, werden wir, der Kürze wegen und um das Schreiben zu complicirter Ausdrücke zu vermeiden, nicht die allgemeinste Function der oben näher bezeichneten Art betrachten, sondern uns auf diejenige besondere dritten Grades beschränken, welche zu der allgemeinsten dieses Grades in ähnlicher Beziehung steht, wie sich für den zweiten Grad die sogenannte Hauptform:

$$x^2 - Dy^2$$

zu der allgemeinen Form:

$$ax^2 + 2bxy + cy^2$$

derselben Determinante verhält. Ist:

$$(5) \quad s^3 + as^2 + bs + c = 0$$

eine cubische Gleichung, deren Coefficienten ganze Zahlen sind, und welche durch keinen rationalen Factor theilbar ist, und bezeichnen:

$$\alpha, \beta, \gamma$$

die Wurzeln derselben, so ist der zu betrachtende Ausdruck:

$$F(x, y, z)$$

das Product von:

$$x + \alpha y + \alpha^2 z$$

und zwei ähnlichen aus β und γ gebildeten linearen Functionen. Die zu lösende Gleichung wird alsdann:

$$(6) \quad F(x, y, z) = m.$$

während die der obigen Gleichung (2) entsprechende mit der folgenden zusammenfällt:

$$(7) \quad F(t, u, v) = 1.$$

Was diese letztere betrifft, so lässt sich durch Betrachtungen, die hier nicht ausgeführt werden können, nachweisen, dass sie wie jene (2) immer auflösbar ist, und es wird nun zu zeigen sein, wie man aus einer oder zwei Auflösungen der Gleichung (7) alle Werthe x, y, z ableiten kann, welche der Gleichung (6) genügen, oder wie man sich davon überzeugen kann, dass keine solche existiren. Hierbei treten nun zwei wesentlich verschiedene Fälle ein, je nachdem nämlich die Gleichung (5) nur eine oder drei reelle Wurzeln hat.

Im ersteren dieser Fälle, den wir allein hier ausführlich besprechen werden, hat die Gleichung (7) mit der Gleichung (2) die Eigenschaft gemein, dass alle

ihre Auflösungen aus einer Fundamental-Auflösung durch Potenziren abgeleitet werden können: allein es ist für unsern Zweck nicht erforderlich, diese einfachste Auflösung zu kennen, sondern das Verfahren bleibt bis auf die grössere Länge der Rechnung ganz dasselbe, wenn man von einer der abgeleiteten Auflösungen ausgeht. Ist nämlich:

$$(T, U, V)$$

eine solche*), und bezeichnet man andererseits mit:

$$X, Y, Z$$

irgend welche ganze Zahlen, die der Gleichung (6) genügen, so lassen sich daraus unendlich viele neue ableiten, wenn man in der Gleichung:

$$(8) \quad x + ay + a^2z = (X + aY + a^2Z)(T + aU + a^2V)^n$$

nach geschehener Entwicklung die rationalen Theile, so wie die Coefficienten von a und a^2 besonders gleich setzt. Die durch diese Formel mit einander verbundenen Auflösungen bilden offenbar wieder eine Gruppe, welche von der Wahl des Anfangsgliedes (X, Y, Z) unabhängig ist, d. h. welche dieselbe bleibt, wenn man dieses mit irgend einem anderen Gliede derselben Gruppe vertauscht. Es folgt daraus, wie oben, dass sich die Gesammtheit aller Auflösungen der Gleichung (6) in solche Gruppen vertheilen lassen muss, und dass man sich im Besitze aller dieser Auflösungen befinden wird, sobald man aus jeder Gruppe ein Glied anzugeben im Stande ist. Nun ist aus (6) und (8) sogleich klar, wenn man unter a diejenige der Wurzeln der Gleichung (5) versteht, welche reell ist, dass:

$$x + ay + a^2z$$

dasselbe Zeichen wie m hat und in jeder Gruppe einmal und nur einmal einen Werth erhält, der zwischen den Grenzen:

$$\sigma \text{ und } \sigma(T + aU + a^2V)$$

mit beliebigem Ausschlusse von einer derselben liegt, wo die Grösse σ ganz willkürlich und der einzigen Beschränkung unterworfen ist, ein dem Zeichen von m gleiches Zeichen zu haben. Die Auffindung aller Auflösungen, welche diese doppelte Bedingung erfüllen und die Repräsentanten von eben so vielen Gruppen sind, lässt sich aber sogleich durch Versuche in endlicher Anzahl

*) Es versteht sich von selbst, dass die ganz illusorische Auflösung $(1, 0, 0)$ ausgeschlossen werden muss.

bewerkstelligen, oder es lässt sich erkennen, dass keine solche und also überhaupt keine Auflösungen der Gleichung (6) existiren. In der That stellt die Gleichung (6), wenn man darin x, y, z als rechtwinklige Coordinaten betrachtet, eine krumme Fläche von unendlicher Ausdehnung dar, welche in unserem Falle, wo nur eine der Wurzeln α, β, γ reell ist, eine Ebene und eine Gerade zu Asymptoten hat. Die oben erhaltenen Ungleichheitsbedingungen haben dann die geometrische Bedeutung, dass man nur das Stück der Fläche zu betrachten hat, welches zwischen den durch die Gleichungen:

$$x + ay + a^2z = \sigma, \quad x + ay + a^2z = \sigma(T + aU + a^2V)$$

bestimmten Ebenen liegt, welche mit der vorher erwähnten Asymptoten-Ebene parallel sind. Dieses Stück aber hat, wie man leicht sieht, nur eine endliche Ausdehnung, so dass man also durch Versuche in beschränkter Anzahl immer wird entscheiden können, welche Punkte desselben ganzzahlige Coordinaten haben, wenn überhaupt Punkte dieser Art vorhanden sind.

Wir bemerken nur noch, dass in dem zweiten der früher unterschiedenen Fälle die Gleichung (7), wie in dem eben besprochenen, unendlich viele Auflösungen zulässt, die aber nicht alle aus einer durch Potenziren abgeleitet werden können. Es existiren vielmehr in diesem Falle zwei Grundauflösungen, welche durch Multiplication und Potenzirung alle übrigen erzeugen. Ohne diese zu kennen, wird es hinlänglich sein, von den derivirten zwei von solcher Beschaffenheit zu haben, dass nicht beide durch Potenzirung in eine und dieselbe dritte übergehen können, um daraus nach einem dem oben angegebenen ähnlichen Verfahren die Gesammtheit aller Auflösungen der Gleichung (6) ableiten zu können.

VERALLGEMEINERUNG EINES SATZES
AUS DER LEHRE VON DEN KETTENBRÜCHEN
NEBST EINIGEN ANWENDUNGEN AUF
DIE THEORIE DER ZAHLEN.

VON

G. LEJEUNE DIRICHLET.

Bericht über die Verhandlungen der Königl. Preuss. Akademie der Wissenschaften. Jahrg. 1842, S. 93—95.

VERALLGEMEINERUNG EINES SATZES
 AUS DER LEHRE VON DEN KETTENBRÜCHEN NEBST
 EINIGEN ANWENDUNGEN AUF DIE THEORIE DER ZAHLEN.

[Auszug aus einer in der Akademie der Wissenschaften am 14. April 1842 gelesenen Abhandlung.]

Ist α ein irrationaler Werth, so giebt es immer unendlich viele zusammengehörige ganze Zahlen x und y , für welche der lineare Ausdruck $x - \alpha y$ numerisch kleiner als $\frac{1}{y}$ ist, wie dies aus der Theorie der Kettenbrüche längst bekannt ist. Die eben ausgesprochene Eigenschaft lässt sich wie folgt verallgemeinern:

„Sind $\alpha_1, \alpha_2, \dots, \alpha_m$ gegebene positive oder negative Werthe von solcher Beschaffenheit, dass der lineare Ausdruck:

$$(1) \quad x_0 + \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_m x_m,$$

in welchem:

$$(2) \quad x_0, x_1, \dots, x_m$$

unbestimmte positive oder negative ganze Zahlen bezeichnen, nur in dem Falle verschwinden kann, wenn $x_1 = x_2 = \dots = x_m = 0$ und also auch $x_0 = 0$ ist, so giebt es immer unendlich viele Systeme (2), worin nicht:

$$x_1 = x_2 = \dots = x_m = 0,$$

und für welche der Ausdruck (1) numerisch kleiner als $\frac{1}{s^m}$ ist, wo unter s der grösste der Zahlenwerthe von x_1, x_2, \dots, x_m verstanden wird.“

Um diesen eben so einfachen als fruchtbaren Satz zu beweisen, wird es genügen nachzuweisen, dass ein System von der verlangten Beschaffenheit gefunden werden kann, für welches ausserdem der numerische Werth von (1) kleiner als eine vorher bestimmte Grösse δ ist. Um ein solches zu erhalten, nehme man eine positive ganze Zahl n , welche die Bedingung:

$$\frac{1}{(2n)^m} < \delta$$

erfüllt, und lege in dem Ausdrücke (1) jeder der Zahlen:

$$x_1, x_2, \dots, x_m$$

alle in der Reihe:

$$-n, -(n-1), \dots, -1, 0, 1, \dots, n-1, n$$

enthaltenen Werthe bei. Bestimmt man nun für jede dieser $(2n+1)^m$ Verbindungen x_0 so, dass (1) einen nicht negativen unter der Einheit liegenden Werth erhält, so hat man $(2n+1)^m$ ächte Brüche, von denen nothwendig wenigstens zwei in *demselben* der durch die Werthe:

$$0, \frac{1}{(2n)^m}, \frac{2}{(2n)^m}, \dots, \frac{(2n)^m - 1}{(2n)^m}, 1$$

begrenzten $(2n)^m$ Intervalle liegen müssen. Zieht man zwei Ausdrücke, denen solche Werthe entsprechen, von einander ab, so erhält man einen neuen Ausdruck von der Form (1), in welchem offenbar *erstens* die Zahlen x_1, x_2, \dots, x_m nicht alle zugleich verschwinden, *zweitens* keine dieser Zahlen, abgesehen vom Zeichen, $2n$ übertrifft, und dessen numerischer Werth endlich *drittens* kleiner als:

$$\frac{1}{(2n)^m} < \delta$$

und also auch kleiner als $\frac{1}{s^m}$ ist.

Hieraus folgt dann sogleich die Existenz von unendlich vielen Systemen (2), welche der Aussage des Satzes entsprechen. In der That, wie viele solcher Systeme man auch als schon bekannt voraussetzen möge, so wird es, da für keines derselben der Ausdruck (1) verschwindet, nach dem eben Gesagten möglich sein, ein neues von den gegebenen verschiedenes zu finden, indem man zu diesem Zwecke nur für δ den kleinsten Zahlenwerth des Ausdrucks (1) zu wählen braucht, welcher einem der schon bekannten Systeme entspricht.

Es giebt analoge Sätze für zwei oder mehr simultane Ausdrücke der Form (1), welche durch dieselben einfachen Betrachtungen erwiesen werden können, und von welchen der auf zwei bezügliche so lautet:

„Sind:

$$\alpha_1, \alpha_2, \dots, \alpha_m$$

und:

$$\beta_1, \beta_2, \dots, \beta_m$$

(wo $m > 2$) zwei Reihen gegebener Werthe von solcher Beschaffenheit, dass die Summen:

$$(3) \quad \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_m x_m,$$

$$(4) \quad \beta_1 x_1 + \beta_2 x_2 + \dots + \beta_m x_m,$$

nur in dem Falle gleichzeitig verschwinden können, wenn:

$$x_1 = x_2 = \dots = x_m = 0$$

ist, so giebt es immer unendlich viele Systeme x_1, x_2, \dots, x_m nicht gleichzeitig verschwindender Zahlen, für welche (3) und (4) resp. numerisch kleiner sind als:

$$\frac{A}{s^a}$$

und:

$$\frac{B}{s^{m-2-a}},$$

in welchen Ausdrücken A und B bestimmte von:

$$\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \beta_2, \dots, \beta_m$$

abhängende und a eine beliebige zwischen 0 und $m-2$ liegende Constante bezeichnen.“

Ein für die Anwendungen auf die Zahlentheorie besonders wichtiger Fall ist der, wo die Exponenten a und $m-2-a$ einander gleich genommen werden und die Ausdrücke in $\frac{A}{s^{\frac{m}{2}-1}}$ und $\frac{B}{s^{\frac{m}{2}-1}}$ übergehen.

Wir fügen noch hinzu, dass diese Sätze und ihre Beweise mit geringen Modificationen auf complexe Zahlen ausgedehnt werden können.

Vermittelst der eben erhaltenen Resultate lässt sich das Lemma, auf welchem die Verallgemeinerung der FERMATSchen Gleichung $t^2 - Du^2 = 1$ beruht, ganz elementar beweisen*), und man sieht zugleich, dass das Lemma, so wie der

*) Comptes rendus des séances de l'Académie des sciences de Paris. Premier semestre 1840, p. 286.¹⁾

¹⁾ S. 622 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

darauf gegründete Satz noch richtig bleibt, wenn die algebraische Gleichung:

$$s^n + as^{n-1} + \dots + gs + h = 0.$$

nur imaginäre Wurzeln hat, vorausgesetzt dass alsdann n grösser als 2 sei. Die in Rede stehende Erweiterung fordert den Nachweis, dass es immer wenigstens *eine* ganze Zahl m giebt, für welche die unbestimmte Gleichung:

$$F(x, y, z, \dots) = m$$

unendlich viele Auflösungen zulässt, und dies folgt mit der grössten Leichtigkeit aus dem ersten oder dem erwähnten besonderen Falle des zweiten der obigen Sätze, je nachdem sich unter den Wurzeln der Gleichung wenigstens eine reelle befindet oder diese sämtlich imaginär sind.

ZUR THEORIE
DER COMPLEXEN EINHEITEN.

VON

G. LEJEUNE DIRICHLET.

ZUR THEORIE DER COMPLEXEN EINHEITEN.¹⁾

[Mitgetheilt in der Sitzung der physikalisch-mathematischen Classe
der Akademie der Wissenschaften am 30. März 1846.]

Es sei:

$$(1) \quad F(\omega) = \omega^n + p_1 \omega^{n-1} + p_2 \omega^{n-2} + \dots + p_n = 0$$

eine Gleichung von beliebigem Grade mit ganzen Coefficienten p_1, p_2, \dots, p_n , die keinen rationalen Factor hat, und deren Wurzeln mit $\alpha, \beta, \dots, \varrho$ bezeichnet werden sollen. Bildet man nun mit n unbestimmten ganzen Zahlen t, u, \dots, z Ausdrücke von der Form:

$$g(\alpha) = t + u\alpha + \dots + z\alpha^{n-1}, \quad g(\beta) = t + u\beta + \dots + z\beta^{n-1}, \quad \dots,$$

so wird das Product:

$$g(\alpha)g(\beta) \dots g(\varrho)$$

eine homogene Function mit ganzen Coefficienten von t, u, \dots, z sein, welche, wie LAGRANGE zuerst bemerkt hat, die merkwürdige Eigenschaft besitzt, sich durch Multiplication und folglich auch durch Potenzirung zu reproduciren. Für die Theorie der so gebildeten Functionen ist nun vor Allem die Beantwortung der Frage, für welche Systeme von Werthen t, u, \dots, z sie der Einheit gleich werden, d. h. die vollständige Auflösung der Gleichung:

$$(2) \quad g(\alpha)g(\beta) \dots g(\varrho) = 1$$

von der grössten Wichtigkeit und als ein Fundamentalproblem dieser Theorie zu betrachten.

Nimmt man gewisse besondere Auflösungen dieser Gleichung aus, welche immer leicht gefunden werden können, und für welche die Factoren:

$$g(\alpha), g(\beta), \dots, g(\varrho)$$

Wurzeln der Einheit sind, so wird jede gegebene Auflösung, zu einer unbestimmten ganzen positiven oder negativen Potenz erhoben, unendlich viele neue Auflösungen erzeugen, und eben so einleuchtend ist es, dass man bei zwei oder mehr gegebenen Auflösungen unbestimmte Potenzen derselben durch Multiplication zu dem-

¹⁾ Die einleitenden Worte im Bericht über die Sitzung lauten: „Hr. Lejeune Dirichlet machte einige Mittheilungen über eine von ihm ausgeführte Untersuchung, welche die Theorie der complexen Einheiten zum Gegenstande hat und nächstens an einem andern Orte bekannt gemacht werden soll“. K.

selben Zwecke verbinden kann. Für den speciellen Fall, wo $F(\omega) = \omega^2 - D$, geht unsere Gleichung in die bekannte PELL'sche Gleichung über, deren sämtliche Auflösungen aus einer Fundamentalauflösung durch Potenziren und Multipliciren mit ± 1 erhalten werden. Es entsteht nun hier die Frage, ob für die allgemeine Gleichung eine ähnliche Eigenschaft stattfindet, und ob auch für diese solche Fundamentalaufösungen existiren, aus welchen durch Potenziren und Multipliciren sämtliche Auflösungen gebildet werden können. Diese Frage findet ihre vollständige Erledigung in folgendem durch seine grosse Allgemeinheit merkwürdigen Satze:

„Bezeichnet h die Gesamtanzahl der reellen und der Paare imaginärer conjugirter Wurzeln der Gleichung (1), so giebt es immer $h-1$ Fundamentalaufösungen von solcher Beschaffenheit, dass, wenn man dieselben potenzirt und in einander multiplicirt und dem so gebildeten allgemeinen Product der Reihe nach jede der vorher erwähnten besonderen Auflösungen als Factor zugesellt, alle Auflösungen von (2) und zwar jede nur einmal dargestellt werden.“

Für die nächsten Grade nach dem zweiten liess sich dieser Satz ohne erhebliche Schwierigkeiten beweisen, und wir haben das auf den dritten Grad bezügliche Resultat in einer früheren Note*) schon vor mehreren Jahren ausgesprochen. Dem Beweise des Satzes in seiner ganzen Allgemeinheit, wie er sich auf dem Wege der Induction bald herausstellte, traten jedoch die grössten Schwierigkeiten entgegen, die erst nach vielen fruchtlosen Versuchen vollständig überwunden werden konnten. Fortgesetzte Beschäftigung mit diesem Gegenstande hat dann endlich den Beweis in solchem Grade vereinfacht, dass wir die Hauptmomente desselben mit wenigen Worten auf eine verständliche Weise zu bezeichnen im Stande sind.

Als der eigentliche Nerv dieses Beweises ist die Auffindung von $h-1$ von einander unabhängigen Auflösungen zu betrachten, unter welcher Benennung wir solche verstehen, die, zu beliebigen Potenzen erhoben und in einander multiplicirt, nie die evidente Auflösung $t = 1, u = 0, \dots, z = 0$ ergeben, ausser wenn sämtliche Potenzexponenten der Null gleich genommen werden. Sind nämlich $h-1$ solche Auflösungen bekannt, so lässt sich vermittelst der in der vorher angeführten Note entwickelten Methode die Gleichung:

$$g(\alpha)g(\beta) \cdots g(\varrho) = r,$$

*) Monatsbericht für October 1841.)

) S. 625 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

in welcher r eine gegebene ganze Zahl bezeichnet, immer vollständig auflösen oder doch zeigen, dass diese Gleichung keiner Auflösung fähig ist. Auf den besonderen Fall angewandt, wo $r = 1$, giebt dieses Verfahren die vollständige Auflösung der Gleichung (2) und nach einigen Umformungen des Resultats gerade in der Form, wie sie unser Satz ausspricht.

Was nun den Nachweis betrifft, dass immer $h-1$ von einander unabhängige Auflösungen existiren, so wird das dazu erforderliche Princip durch gewisse allgemeine Sätze an die Hand gegeben, die eine merkwürdige Verallgemeinerung der Eigenschaften der Kettenbrüche darbieten und der Akademie schon vor vier Jahren mitgetheilt worden sind*). Mit Hülfe dieser Sätze kann man immer eine Auflösung der Gleichung (2) finden, für welche der Zahlenwerth jedes der Ausdrücke $q(\alpha)$, $q(\beta)$, ..., $q(\varrho)$, die reellen Wurzeln entsprechen, so wie jedes Product von je zweien, zu conjugirten imaginären Wurzeln gehörenden nach Belieben unter oder über der Einheit liegt, wenn man nur die zwei offenbar unmöglichen Combinationen ausschliesst, wo alle zugleich grösser oder alle zugleich kleiner als die Einheit sein sollen. Ist dieser Punkt erst erledigt, so lässt sich das über die unabhängigen Auflösungen Behauptete wie folgt zeigen.

Bezeichnet man für eine gegebene Auflösung mit:

$$a, b, \dots, k$$

diejenigen der Ausdrücke $q(\alpha)$, $q(\beta)$, ..., $q(\varrho)$, welche reell sind, so wie die Producte von je zwei zusammengehörigen imaginären, so hat man:

$$ab \dots k = 1.$$

Sollen nun z. B. drei Auflösungen, für die wir a, b, \dots, k mit den Indices 1, 2, 3 versehen wollen, unabhängig von einander sein, so muss die Gleichung:

$$a_1^{m_1} a_2^{m_2} a_3^{m_3} = 1$$

nicht anders bestehen können, als wenn die ganzen Zahlen m_1, m_2, m_3 gleichzeitig verschwinden. Berücksichtigt man, dass diese Gleichung, wenn sie stattfindet, nicht aufhören wird, richtig zu sein, wenn man a in b oder c verwandelt, und bezeichnet mit den grossen Buchstaben die Logarithmen der Zahlenwerthe der durch die entsprechenden kleinen ausgedrückten Grössen, so sieht man, dass die Bedingung für die Unabhängigkeit der drei Auflösungen darin besteht, dass die drei linearen Gleichungen:

*) Monatsbericht für April 1842.¹⁾

¹⁾ S. 633 dieser Ausgabe von G. Lejeune Dirichlet's Werken. K.

$$A_1 m_1 + A_2 m_2 + A_3 m_3 = 0, \quad B_1 m_1 + B_2 m_2 + B_3 m_3 = 0, \quad C_1 m_1 + C_2 m_2 + C_3 m_3 = 0$$

keine andere Auflösung in ganzen Zahlen zulassen dürfen als:

$$m_1 = 0, \quad m_2 = 0, \quad m_3 = 0.$$

Diese Bedingung wird aber offenbar erfüllt sein, wenn die sogenannte Determinante aus den neun Coefficienten oder nach der üblichen Bezeichnung der Ausdruck:

$$\Sigma \pm A_1 B_2 C_3$$

von Null verschieden ist, da alsdann die Gleichungen nur auf die angegebene Weise erfüllt werden können, selbst wenn man davon abstrahirt, dass m_1, m_2, m_3 ganz sein sollen.

Durch dieses Resultat, in Verbindung mit dem vorher erwähnten, ist nun ein Mittel gegeben, die Anzahl der unabhängigen Auflösungen allmählich zu vergrössern, bis sie gleich $h-1$ geworden ist. Um z. B. zu drei bekannten, für welche $\Sigma \pm A_1 B_2 C_3$ von Null verschieden ist, eine vierte hinzuzufügen, hat man nur A_4, B_4, C_4, D_4 so einzurichten, dass $\Sigma \pm A_1 B_2 C_3 D_4$ ebenfalls nicht verschwinde. Nun ist aber bekanntlich:

$$\Sigma \pm A_1 B_2 C_3 D_4 = D_4 \Sigma \pm A_1 B_2 C_3 + C_4 F + B_4 G + A_4 H,$$

wo F, G, H nichts die nun hinzukommende Auflösung Betreffendes enthalten. Giebt man jetzt D_4 dasselbe Zeichen, welches $\Sigma \pm A_1 B_2 C_3$ hat, und C_4, B_4, A_4 resp. die Zeichen von F, G, H , falls sie nicht verschwinden, so ist die zweite Seite und also auch die erste positiv, d. h. die neu hinzugekommene Auflösung bildet mit den drei schon vorhandenen ein System unabhängiger Auflösungen.

Wir bemerken zum Schlusse noch, dass die Untersuchungen, über welche wir so eben einige Andeutungen gegeben haben, mittelst derselben Principien einer viel grösseren Ausdehnung fähig sind, als denselben hier gegeben worden ist. Man kann, statt wie es hier geschehen ist, nur *eine* Gleichung zu Grunde zu legen, mehrere Gleichungen betrachten, und die Factoren der zu bildenden Function aus den einzelnen Combinationen der Wurzeln dieser Gleichungen zusammensetzen, so wie man auch andererseits statt der ganzen Zahlen, welche als Coefficienten oder als Variablen der homogenen Function vorkommen, complexe Zahlen einer beliebigen Form einführen kann. Auf alle diese Erweiterungen bleiben dieselben Principien anwendbar, was das günstigste Zeugniß dafür ablegt, dass diese Principien dem wahren Wesen des Gegenstandes entnommen sind.

(2) 2015 4

(1)

QA Lejeune-Dirichlet, Peter
3 Gustav
L34 Werke
Bd.1

Physical #
Applied Sci

PLEASE DO NOT REMOVE
CARDS OR SLIPS FROM THIS POCKET

UNIVERSITY OF TORONTO LIBRARY
